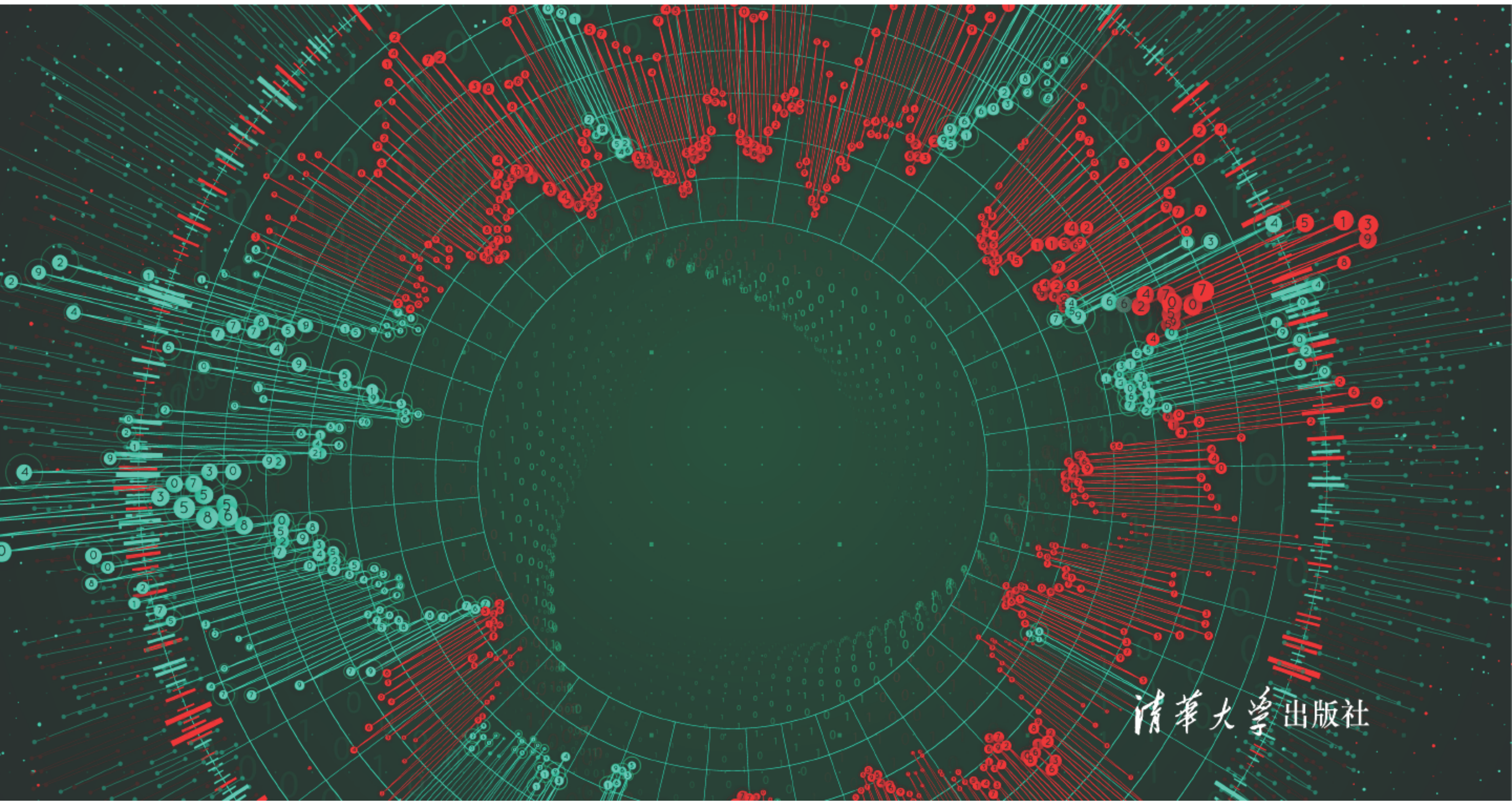
量子计算机

穿越未来世界

李联宁◎编著

了解量子力学和未来计算机，
从这本书开始

- 量子技术是近年来发展的前沿技术领域，**大数据搜寻、破译密码、机器学习、人工智能、身份识别**都是量子计算擅长的方向。
- **量子计算**和**量子通信可以解决经典计算机无法解决的问题**，5年内将会出现相应的商业化运用，10年内会有普遍性的运用。
- 本书**适用于所有对量子计算机**领域感兴趣、具有强烈求知欲和希望走进未来世界的读者。



清華大学出版社

VISIT…

LANZAROTE
Caliente.COM

量子计算机

——穿越未来世界

李联宁　编著

清华大学出版社
北　京

内容简介

量子技术是近年来发展的前沿技术领域，大数据搜寻、破译密码、机器学习、人工智能、身份识别都是量子计算擅长的方向。无论是量子计算还是量子通信，目的都在于解决经典计算机无法解决的问题。预计，5年内将会出现相应的商业化运用，10年内会有普遍性的运用，国内外都很关注这一技术的发展。

本书以浅显易懂的方式讲解复杂的技术前沿问题，避免使用高深的量子力学、高等数学、计算机原理专业知识，深入浅出地详细介绍量子计算机的基础理论、最新技术。

本书按量子计算机发展阶段和不断扩展的应用范围依次介绍了涉及量子计算与通信的相关理论基础、量子计算、量子通信与网络、量子安全与密码系统、行业案例研究、量子技术发展前景。

近年来，量子技术有长足的发展，量子计算机与量子通信已经出现在未来世界的门口，目前国内图书市场上开始出现一些量子科学技术书籍，但主要是国外原版专著或其译本，大多数对应于研究生教学层次。为适应广大对现代技术有浓厚兴趣的读者的需求，作者编著了这本量子计算机入门科普书籍，必要时也可作为各级院校的专业教材。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

量子计算机：穿越未来世界／李联宁编著. —北京：清华大学出版社，2019
ISBN 978-7-302-52305-5

Ⅰ. ①量…　Ⅱ. ①李…　Ⅲ. ①量子计算机－普及读物　Ⅳ. ①TP385-49

中国版本图书馆CIP数据核字（2019）第029201号

责任编辑：白立军
封面设计：杨玉兰
责任校对：梁　毅
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：20.5　　**字　　数**：349千字
版　　次：2019年9月第1版　　**印　　次**：2019年9月第1次印刷
定　　价：49.00元

产品编号：079354-01

前　言

先问大家如下三个问题。

第一个问题，在世界IT行业最著名的与比尔·盖茨齐名、自学中文成才的华人女婿是谁？凡是IT行业的人纷纷举手，是Facebook（脸书）创始人兼首席执行官马克·扎克伯格。对！

第二个问题，马克·扎克伯格的孩子是男孩还是女孩？一半的人举手，女孩。有人还补充说，马克·扎克伯格准备在孩子长大以后把自己的99%的资产裸捐出去。对！

第三个问题，谁看过马克·扎克伯格抱着女儿读一本书的照片？只有25%的人有印象。如果我再加深一点，读的书的书名是什么？绝对没有人注意过！

我告诉你，书名是 *Quantum Physics for Babies*，翻译成中文，书名就是《给宝宝的量子物理学》。有人问，这是她应该学的东西吗？马克·扎克伯格的回答是“不管她未来想做什么，做老师也好，像她妈妈那样，做医生也好，或者她想从事自己的事业，我希望她都能有这样的求知欲。求知欲就是我想知道为什么，以及我为什么不能做得更好。”

受马克·扎克伯格的启发，作者编写了下面这么一本书，全书分三部分。

第一部分　基础理论及概念，包括第1章～第4章。

第二部分　量子计算与通信部分，包括第5章和第6章。

第三部分　量子技术安全与应用技术部分，包括第7章和第8章。

在这本书里，你可以发现以下内容。

- 苹果有没有真正落在牛顿头上？
- 计算机怎么和力学搞到一起了？

- 原来我们反复学过的物理只是解释了宏观世界的规律,一到微观世界就不灵了。
- 挑战量子力学的带头大哥就是爱因斯坦!
- 爱因斯坦的“鬼魅学说”——量子纠缠。
- 千里之外的心灵感应——隐形传输。
- 量子隐形传态是“嗖”的一声把人传过去的瞬间传输吗?
- 量子密码的鼻祖——海森伯测不准原理。
- 所有计算机(包括量子计算机)的同一祖宗——图灵机。
- 我们说的“量子比特”不是“比特币”。
- 为什么当今所有的密码系统都失效了。
- 信息化战争:量子计算的意义不亚于核武器。
- 传统计算机渐渐接近它们的极限,近20年芯片的发展速度几乎没有提升!
- 量子计算机真的来了,全球第一台商用型量子计算机售价1500万美元。
- 在量子计算机给予一种新的计算能力水平的同时,IT工程师会失业吗?

书名考虑选为《量子计算机——穿越未来世界》,其含义有两个层次:

第一,作为量子计算及通信的入门科普书籍;

第二,作为未来10～20年IT行业技术进步的入门基础知识储备教科书。

本书献给所有具有强烈求知欲和希望走进未来世界的朋友们,谢谢您看完以上这段文字。

编　者

2019年3月

目　录

第 1 章　漫话：量子计算机来了 ……………………………………………… 1

1.1　量子技术的前世今生 ……………………………………………… 1

　　1.1.1　先说说什么是量子 ……………………………………………… 1

　　1.1.2　宏观世界和微观世界是那么的不同 ……………………………… 2

1.2　世界上最小的“东西”是量子 ……………………………………… 3

　　1.2.1　分子、原子和量子，哪个最大？哪个最小 ………………………… 3

　　1.2.2　量子计算机是什么 ……………………………………………… 7

　　1.2.3　量子计算将在我们有生之年普及 ……………………………… 11

1.3　计算机和力学 ……………………………………………………… 12

　　1.3.1　量子力学与现实生活有什么联系 ……………………………… 12

　　1.3.2　什么是量子力学 ………………………………………………… 13

　　1.3.3　全新的计算理论诞生 …………………………………………… 16

1.4　10 分钟看懂量子比特、量子计算和量子算法 ……………………… 16

　　1.4.1　波粒二象性 ……………………………………………………… 17

　　1.4.2　量子纠缠 ………………………………………………………… 17

　　1.4.3　量子叠加 ………………………………………………………… 18

　　1.4.4　量子比特和量子计算 …………………………………………… 21

1.5　量子计算机是什么计算机 ………………………………………… 24

　　1.5.1　什么是量子计算机 ……………………………………………… 24

1.5.2 量子计算机的前世今生 …… 25
1.5.3 量子计算机进入世界级竞赛 …… 27
1.6 未来世界是量子互联网的时代 …… 33
1.7 现在最火的是量子通信 …… 35
1.7.1 量子通信卫星怎么样给小明发送密码 …… 35
1.7.2 最火的颠覆性技术量子通信在中国 …… 37
1.8 通信编码需要大智慧 …… 39
1.8.1 解说通信编码 …… 39
1.8.2 我要说的是“悄悄话” …… 40
1.9 当今所有密码系统都失效了 …… 44
1.9.1 量子加密的“不破金身” …… 44
1.9.2 走近“颠覆性技术”——量子通信能否取代传统通信 …… 46
第2章 计算机祖孙三代 …… 47
2.1 计算机爷爷——图灵机模型 …… 47
2.1.1 艾伦·图灵是个科学家 …… 47
2.1.2 图灵机模型 …… 49
2.1.3 计算机界的诺贝尔奖 …… 50
2.2 所有计算机的同一祖宗——图灵机 …… 50
2.3 计算机爸爸——冯·诺依曼机 …… 53
2.3.1 第一个“攒”计算机的人——冯·诺依曼 …… 53
2.3.2 经典计算机的五脏六腑 …… 55
2.3.3 经典计算机的工作“门道” …… 57
2.4 计算机孙子——量子计算机 …… 60
2.4.1 量子计算机的起源 …… 60
2.4.2 量子计算机的研究历史 …… 61

2.4.3 量子计算机算法理论 …… 62
2.5 量子计算机的“硬件单元”已经造出来了 …… 66
2.5.1 量子计算机的硬件单元 …… 67
2.5.2 量子计算机的硬件逻辑单元是用什么材料做成的 …… 71
2.5.3 新型量子计算机首个基本元件问世 …… 72
2.5.4 世界上第一个完整的量子计算机芯片设计揭晓 …… 73
2.6 量子计算机里面还得有“软件算法” …… 74
2.6.1 量子计算机的算法理论 …… 74
2.6.2 为量子计算机量身定做的 Shor 算法 …… 75
2.6.3 量子并行计算的随机搜索——Grover 算法 …… 76
2.7 量子计算机展望 …… 77

第 3 章 牛顿力学的困境及飞跃 …… 82

3.1 物理大家族 …… 82
3.1.1 经典物理学的建立发展过程 …… 82
3.1.2 物理学的危机 …… 83
3.1.3 经典物理学的完成和局限 …… 85
3.1.4 量子论的出现 …… 87
3.2 家族长子：牛顿力学 …… 89
3.2.1 苹果为什么会落在牛顿头上 …… 89
3.2.2 牛顿是谁 …… 91
3.2.3 牛顿想的也对也不对：适用范围与局限性 …… 93
3.3 家族长孙：量子力学 …… 97
3.3.1 量子力学漫谈 …… 97
3.3.2 量子力学是用来解释微观粒子的物理分支 …… 100
3.3.3 “薛定谔猫”的困境 …… 102

3.3.4　量子世界中，波函数到底是数学描述还是实体 …… 104
3.3.5　搞量子力学没点高数基础不行——薛定谔方程 …… 106
3.3.6　眼见为实：量子力学的实验证明 …… 108
3.3.7　牛顿力学与量子力学的决战 …… 113
3.4　独门绝活：量子纠缠 …… 119
3.4.1　给量子纠缠做个 CT …… 119
3.4.2　千里之外的心灵感应：隐形传输 …… 124
3.4.3　量子纠缠将远程控制你的生活 …… 127
3.5　川剧变脸：量子态套叠 …… 128
3.5.1　一般人都搞不清楚的量子态套叠 …… 128
3.5.2　原来如此：量子态套叠原理 …… 129
3.6　挑战量子力学的带头大哥——爱因斯坦 …… 129
3.6.1　量子力学描述世界的语言跟经典力学有根本区别 …… 129
3.6.2　EPR 实验 …… 131
3.6.3　泊松亮斑 …… 133
3.6.4　量子隐形传态是“嗖”的一声把人传过去的瞬间传输吗 …… 133

第 4 章　量子信息脸谱 …… 137

4.1　什么是量子信息 …… 137
4.1.1　量子信息三兄弟 …… 137
4.1.2　量子信息学 …… 139
4.2　量子比特不是比特币 …… 140
4.2.1　比特币 …… 140
4.2.2　量子比特 …… 141
4.3　量子信息的身世 …… 143
4.3.1　量子信息的源头 …… 143

4.3.2 量子信息技术的发展 …… 145
4.3.3 小有小的规矩——量子编码定理和量子编码方案 …… 147
4.4 这个“比特”和那个“比特”不一样 …… 149
4.4.1 风光无限“大哥大”——经典比特 …… 149
4.4.2 领跑下一代——量子比特 …… 150
4.4.3 量子比特叠罗汉 …… 151
4.4.4 谨防“李鬼”！基于量子比特原理才叫量子产品 …… 152

第5章 未来世界的大佬——量子计算 …… 155

5.1 量子计算 …… 156
5.1.1 量子计算的发展历程 …… 156
5.1.2 量子计算的基本原理 …… 157
5.1.3 量子计算机的实现 …… 159
5.1.4 光量子计算机 …… 161
5.2 量子计算的黑白两道 …… 162
5.2.1 白道：量子叠加性 …… 162
5.2.2 黑道：量子相干性 …… 168
5.3 量子计算独门绝技：量子算法 …… 170
5.3.1 高等数学＋：基于 Shor 分解大数质因子量子算法 …… 171
5.3.2 百度一下：基于 Grover 量子搜索算法 …… 172
5.3.3 量子智能计算 …… 173
5.4 量子计算机的细胞核：门电路 …… 173
5.4.1 华山论剑门派一：量子逻辑门 …… 176
5.4.2 华山论剑门派二：单量子比特门 …… 180
5.4.3 华山论剑门派三：条件非门 …… 181
5.4.4 华山论剑门派四：量子芯片 …… 183

5.4.5 华山论剑门派五：量子传感器 …… 184
5.5 最火的量子计算机来了 …… 185
5.5.1 众说纷纭的理论及研究 …… 185
5.5.2 信息化战争：量子计算的意义不亚于核武器 …… 189
5.5.3 分久必合：量子计算机的工作原理 …… 191
5.5.4 合久必分：IT 世界顶级高手的竞争 …… 197
第 6 章 未来世界的神经中枢——量子通信 …… 203
6.1 未来世界的神经系统 …… 203
6.1.1 改变世界的新技术：量子通信 …… 203
6.1.2 众人拾柴火焰高：量子通信的类型 …… 206
6.2 云中漫步——量子隐形传态 …… 207
6.2.1 通信神话：量子隐形传态的原理 …… 207
6.2.2 原来是真的：量子隐形传态实验 …… 209
6.3 风靡全球——量子信道 …… 211
6.3.1 未来世界的高速公路：量子信道 …… 211
6.3.2 能比光还快吗：光纤量子信道 …… 214
6.3.3 太空通信：自由空间量子信道 …… 217
6.4 给互联网插上量子的翅膀——量子通信 …… 219
6.4.1 通向未来的网络：量子通信网络的体系结构 …… 219
6.4.2 未来世界的互联互通：量子通信网络中的交换技术 …… 224
6.4.3 世界太大了：量子中继器 …… 236
6.4.4 量子通信产业链 …… 238
第 7 章 量子世界的‘看门狗”——安全及密码 …… 241
7.1 “看门狗”的祖宗：经典密码学与现代密码学 …… 241

7.1.1 古罗马人的密信：经典密码学 …… 242
7.1.2 德国人第二次世界大战时使用的密码机：现代密码学 …… 243
7.2 量子密码的鼻祖：海森伯测不准原理 …… 248
7.2.1 海森伯不确定原理 …… 248
7.2.2 测不准原理所起的作用 …… 250
7.3 我的地盘我做主：量子密码学 …… 251
7.3.1 量子密码的起源与发展 …… 251
7.3.2 量子密码技术的原理 …… 252
7.4 Alice 和 Bob 的对话：量子密钥分发 …… 257
7.4.1 量子密钥分发 …… 258
7.4.2 BB84 量子密钥分发协议及其工作原理 …… 259
7.4.3 量子保密通信进展以及墨子星 …… 263
7.4.4 我怎么知道有人在偷听：光子的偏振态 …… 266
7.5 量子密码的宝典——工作原理 …… 269
7.5.1 宝典一：量子密码理论模式 …… 269
7.5.2 宝典二：量子密码理论分析 …… 271
7.5.3 宝典三：量子密码假设 …… 271
7.6 人人都有的秘密——量子密钥分发 …… 273
7.6.1 量子密钥分配的远程通信 …… 273
7.6.2 云中漫步安全保障：量子保密通信系统 …… 273
7.7 量子安全直接通信 …… 275

第8章 量子计算机的“社会分工” …… 277

8.1 世界是我们的也是你们的：传统计算机渐渐接近它们的极限 …… 277
8.1.1 近20年芯片的发展速度几乎没有提升 …… 277
8.1.2 登纳德定律中一直在“偷懒”的芯片 …… 280

8.1.3 多核的陷阱：从程序的角度探讨计算机的极限 …… 284
8.1.4 量子计算机：误解带来的乐观与恐慌 …… 287
8.2 量子计算机赋予计算机一种新的计算能力水平 …… 292
8.2.1 我们为什么需要量子计算 …… 292
8.2.2 量子计算机要从囚禁原子开始 …… 297
8.2.3 必须“冷酷”的量子计算机 …… 298
8.2.4 量子计算机研制面临的技术困难 …… 304
8.2.5 量子计算机会不会取代今天的计算机 …… 305
8.2.6 量子计算机最终什么时候实现 …… 308
8.2.7 如果量子计算机被推广，我们会失业吗 …… 309
参考文献 …… **313**

第1章

漫话：量子计算机来了

1.1　量子技术的前世今生

1.1.1　先说说什么是量子

量子究竟是什么?

我们知道,构成物质的最小单元是基本粒子,而量子就是质量、体积、能量等各种物理量的最小单元,而且它也要以某种粒子状态存在。简单地讲,量子不是粒子,它是计量能量的最小单位。

最早,量子是被一个叫普朗克的德国物理学家(如图 1-1 所示) 在 1900 年提出来的,后来陆陆续续经过许多科学家的努力,其中也包括大名鼎鼎的爱因斯坦,使得量子科学体系不断完善。

图 1-1　德国物理学家普朗克

如果用通俗的话描述量子，就可以这么理解：世界上，有些东西是连续的，例如打

开水龙头，有水流出来，根据水龙头打开的大小，水流可以连续地发生变化。但有些东西就不能这样了，例如机枪，射出的子弹就不能连续变化，要么一个，要么两个，总之是 n 个，n 只能是整数，你用机枪发射 1/2 个子弹试试？

平常，人们看到的物质是由原子组成的，可是原子世界的运动规律与宏观世界完全不同。例如，原子的能量不是连续变化的，而是一份一份的，物理学家就把其中最小的一点点分量叫作量子。后面讲到的，当今最火的量子通信就是利用这种规律做出来的通信技术。

科学家发现，光线也是不连续的，而是由一个一个光子组成的，人们称之为光量子。研究量子的科学，叫量子力学。随着研究的深入，科学家发现，微观世界的各种基本粒子，无一例外，都服从量子力学的规律，这些规律和人们日常所见的宏观世界的规律大相径庭，这让人们瞠目结舌，困惑不解。

1.1.2 宏观世界和微观世界是那么的不同

宏观世界与微观世界是那么的不同，例如，在宏观世界，波和粒子是不同的概念，但在微观世界，两者可以统一起来。例如光线，既可以看成是波——光波，又可以看成是粒子——光子，具有“波粒二重性”。

当爱因斯坦第一次提出光的“波粒二重性”的时候，遭到大多数人的嘲笑和攻击：什么意思？每周 1、3、5 是波，2、4、6 是粒子，轮流坐庄？这不是胡说八道吗？

然而，实验证明，爱因斯坦是对的：任何时候，光都有波粒二重性。人们理解不了，也没有办法，只能慢慢理解吧。

还有，在宏观世界，一个物体的速度和位置，是可以同时准确测定的，例如飞机来了，雷达可以把飞机的速度、位置都准确测定。但对于微观粒子，就不行了，科学家发现，如果把一个基本粒子的位置测准了，它的速度就测不准了。还有，时间和能量，也只能测准其中之一。这就是著名的“测不准原理”。

顺便说一句，在微观世界，测量可不是一件简单的事，测量会破坏或改变微观粒子的状态。

还有一种难以理解的现象，就是量子纠缠。

如果把两个基本粒子“纠缠”起来（如何纠缠后面再讲），然后把这两个粒子分开，一个放在北京，一个放在上海，当你改变北京那个粒子的状态时，上海那一个粒子的状态也会同时改变，尽管它们之间没有发生任何联系。

这种“超距作用”的传播距离，还可以更远，理论上，即使两个粒子相隔若干光年，例如一个放在地球上，另一个放到织女星上，也是可以相互影响的。

这种现象，在历史上被爱因斯坦称为“鬼魅学说”，他认为违反了因果律和定域性原则，是不可信的，为此，他和量子力学的代表人物——丹麦物理学家玻尔，争论了很多年。

但是，近年来越来越多的实验证明，爱因斯坦可能错了。

2015年10月25日，荷兰代尔夫特理工大学的科学家们把两颗钻石分别放在代尔夫特理工大学校园内的两侧，距离1.3km。每块钻石含有一个可以俘获单个电子的微小空间，每个空间放置一个被纠缠过的电子，它们之间，没有任何方式的联系。实验证明，确实存在这种奇异的“超距作用”，改变其中一个的状态，另一个的状态也发生了改变。

1.2　世界上最小的“东西”是量子

1.2.1　分子、原子和量子，哪个最大？哪个最小

分子是由原子组成的。分子最大，量子最小。这三者之间有没有什么关系呢？

大家在上中学的物理和化学课时就知道：

质子 ＋ 中子 ＝ 原子核；

原子核 ＋ 电子 ＝ 原子；

原子 ＋ 原子 ＝ 分子；

原子失去或得到部分电子，就是离子。

至于等离子，这么说吧，带正电和负电的粒子，如原子核和电子，在一块，但又不组成原子，分散存在，这种状态叫作等离子状态，这种物体叫作等离子体。

总结一下，物质是由分子构成，分子是由原子构成，原子是由更小的粒子——质子、中

子和电子构成。后来又有中微子、夸克。如今人类科技发现最小的粒子还有重子、强子、介子及超子等。基本粒子的结构关系与尺寸关系如图 1-2 所示。

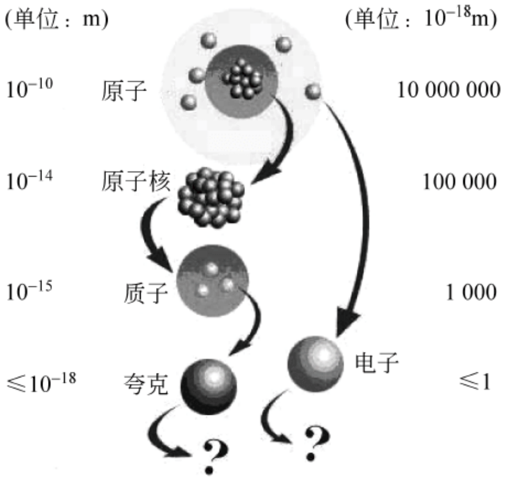

(单位：m)
(单位：10^{-18}m)
10^{-10}
原子
10 000 000
10^{-14}
原子核
100 000
10^{-15}
质子
1 000
$\leqslant 10^{-18}$
夸克
电子
$\leqslant 1$
?
?

图 1-2 基本粒子的结构关系与尺寸关系

如果你说搞不清楚，一定是上课睡觉梦见周公去了，可以考虑重新再上一回物理课。

1. 原子

原子(atom)指化学反应不可再分的基本微粒，原子在化学反应中不可分割，但在物理状态中可以分割。原子由原子核和绕核运动的电子组成。原子是构成一般物质的最小单位，同类原子统称为元素。已知的元素有 118 种。

2. 质子

质子(proton)是一种带 1.6×10^{-19}C(库仑)正电荷的亚原子粒子，大约是电子质量的 1836.5 倍。原子核中质子数目决定其化学性质和它属于何种化学元素。

世界上原子不是最小的量子(量子是能量的单位)，质子是带正电的小微粒，就是小粒子，中子是不带电的小粒子，两者都非常小。电子是带负电的小粒子，比质子和中子还小。光是由粒子构成的，每个粒子就叫作光子。

3. 夸克

夸克(quark)是一种参与强相互作用的基本粒子，也是构成物质的基本单元。夸克互

相结合，形成一种复合粒子，叫强子。强子中最稳定的是质子和中子，它们是构成原子核的单元。由于一种叫“夸克禁闭”的现象，夸克不能够直接被观测到，或是被分离出来，只能够在强子里面找到。基于这个原因，人们对夸克的所知大都是间接地来自对强子的观测。

4. 量子

量子(quantum)是现代物理中的重要概念。量子不是粒子，它是计量能量的最小单位。

量子最早是普朗克在1900年提出的。他假设黑体辐射中的辐射能量是不连续的，只能取能量基本单位的整数倍。后来的研究表明，不但能量表现出这种不连续的分离化性质，其他物理量诸如角动量、自旋、电荷等也都表现出这种不连续的量子化现象。这与以牛顿力学为代表的经典物理有根本的区别。量子化现象主要表现在微观物理世界。描写微观物理世界的物理理论就是量子力学。

原子、分子、原子团、蛋白质这些微观的东西都属于量子力学研究的范畴。因为经典力学的定理和定律在这些微观的东西上都不适用。物理基本划分为三大块：研究微观物质的量子力学，研究现实平常东西的经典力学和研究强引力、高速度的天文学。

5. 量子与质子、原子之间的关系

其实量子的概念是把物质整数化(而不是小数化)，不存在连续可分性，诸如有些人认为10cm的一半是5cm，5cm的一半是2.5cm，按道理你可以无限次分下去，但是量子的概念告诉我们这样分是有尽头的。

在物理学中，一个量如果不能连续变化，只能取一些分立的值，我们就说它是量子化的。好比上台阶，只能上一个台阶，而不能上半个。宏观世界里的物理量似乎都能连续变化，但在微观世界，许多物理量是量子化的。例如氢原子中电子的能量只能取一个基本值——13.6eV或者取其1/4、1/9、1/16、1/25等，而不能取其2倍或1/2、1/3。

6. 量子力学

量子力学描述世界的语言与经典力学有根本区别。经典力学描述一个物体的状态，会给出它的明确位置；量子力学描述一个微观粒子的状态，给出的则是叠加态——这个粒

子在某些情况下既可能在这里，也可能在那里，没有确定的位置。好比孙悟空的分身术，一个孙悟空能够同时出现在多个地方，孙悟空的各个分身就像是他的叠加态。

举一个非常浅显的例子，在提款机你可以提 100 元、200 元、300 元等，这些都是 100 的倍数，不可以提 105 元或 105.5 元，因为提款机只出纸币，而不出硬币，105 元或 105.5 元对提款机是没有意义的，不是说这个世界没有 105 元！只是提款机不能处理零钱。量子世界也是这样被量子化（quantization），在提款机上取出的钱都是 100 的倍数，而类似光子波长，我们用 4000Å、4001Å 等表示，它们都是 1Å 的倍数，是不是说没有 4000.5Å 波长的光呢？不是，只不过在量子力学中没有意义，波长只可以量子跃迁（quantum leap）的方法改变，它必须是某一个基本单位（例如 1Å）的整数倍数。

7. 量子与原子、电子之间的不同

一个物理量如果有最小的单元且不可连续分割，就说这个物理量是量子化的，并把最小的单元称为量子。重要的事情说三遍，量子不是粒子，它代表最小单位的能量！

其基本概念是所有的有形性质也许是“可量子化的”。“量子化”指其物理量的数值会是一些特定的数值，而不是任意值。例如，在“休息状态”的原子中，电子的能量是可量子化的，这能决定原子的稳定和一般问题。最小的能量值是一个能量子，它的数值，就是一个普朗克常量。构成光的最小能量叫光子。

以前研究的人发现能量的传递不是连续的，不是说想传递任意值的能量就能传递任意值的能量。人们发现能量的传递是一个数值的整数倍。发现能量也有小到不可再分的一份，必须得按这一份的整数倍传递。如果有类似温度计一样的能量计量装置，把它放大到能看到整个细节的时候，你会发现里面的“水银”不是像我们平常感觉到的连续下落，而是快速、一格一格地往下掉。一格就是一个量子。

当接触到能量子后，就不再有连续的概念。量子作为宇宙中最小的能量，一切东西都以量子的整数倍存在，没有变化是连续的。将现实世界以量子的眼光看，没有比量子还小的位移。你从这里走到那里，好像整个过程没有一个地方落下，其实你的身体动作都是一格一格地位移。你与人说话，感觉自己嘴唇是连续动，其实慢放到量子级。你的嘴唇是在一格一格地动。而格与格之间你并没接触过，也没有连续的线，那儿只是一个很密的点

集，点与点之间距离最小为量子的点集。也没有连续的时间与空间。数学函数里的连续在现实中是讲不通的。将函数图像量子化，函数都是点集，哪来的连续？

8. 量子存在于原子哪里

量子是种广泛的概念，而不是一种具体的粒子。前面已经说过，量子不是粒子，它是计量能量的最小单位。量子力学认为物质（包括时空）都不是连续的，而是一份一份的，连电磁波也是一份一份的，即光量子。

1.22　量子计算机是什么

1. 量子计算机使用量子比特

量子计算机依赖出现在自然界的量子力学现象——基本上是物质的两种重要状态，名为叠加（superposition）和纠缠（entanglement）。物质的这些状态被用于计算时，有望提升对复杂数据集执行计算的能力。

这里的重要区别在于量子计算机不同于传统计算机，传统计算机是依赖晶体管的二进制数字电子计算机。

什么是晶体管？这个估计大家都知道，普通智能手机里面就有几十万个晶体管，晶体管可在两种状态之间切换：0 或 1，即开或关，从而计算信息。

量子计算机并不使用晶体管（或经典比特），而是使用量子比特（Qubit）。经典比特与量子比特的区别如图 1-3 所示。

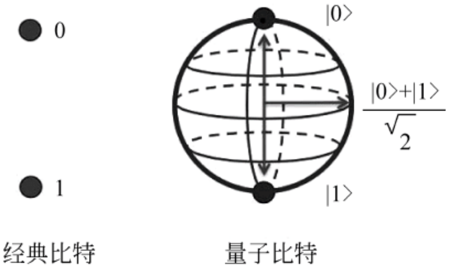


图 1-3　经典比特与量子比特的区别

量子比特是量子计算机中基本的信息单位。

量子比特可能是－1 或 1，也就是同时拥有这两个值的属性，这就叫叠加。所以，执行计算方面立即有了更多种可能性。

如今市面上最先进的量子计算技术可以使用多达 1000 量子比特。

另外，量子比特可以利用一种名为量子纠缠的状态，在这种状态中，成对或成组的量子粒子连接起来，那样每个粒子就无法独立于其他粒子加以描述，即便粒子之间隔着很远的距离（例如宇宙的两端）。

爱因斯坦称之为“远距离的幽灵行动”（spooky action at a distance），它正是量子传输的理论基础。

对于那些不是量子物理学家的普通人来说，重要的是，由于量子比特以及叠加和纠缠现象，量子计算机可以同时处理大量计算任务，而且速度比传统计算机快得多。

2. 量子技术的实际应用

首先，不妨来一个思维实验。设想一下你手拿一本电话簿，然后再设想你要在该电话簿中查询某个特定的电话号码。使用晶体管的经典计算机会搜索电话簿的每一行，直至找到并返回匹配号码。相比之下，由于拥有量子比特，量子计算机可以同时评估每一行，并返回结果，速度比经典计算机快得多，可以立即搜索整本电话簿。

因此，该技术可以应用于那些有无限变量的行业问题，那些变量组合构成一系列数量非常多的潜在解决方案。这些巨大的变量问题通常被称为优化问题。

例如，可以为中国每个春节回家过年的人（要知道，这是每年人类的最大迁徙）优化航线、机场时刻表、天气数据、燃料成本和乘客信息等，从而获得全中国总体来说最具有成本效益的解决方案。经典计算机需要几千年时间计算解决这个问题的最佳方案。从理论上说，每台量子计算机的量子比特数量增加后——这一幕已成为现实，量子计算机就可以在几小时内或更短时间内完成这项任务。

量子比特的发展速率以时间为轴，速度呈线性上升，如图 1-4 所示。

3. 量子计算机已经造出来了

加拿大 D-Wave 公司在几年前已经制作出世界上第一台商用量子计算机 D-Wave Systems，位于加拿大温哥华的量子计算机如图 1-5 所示。这家公司被广泛视为量子计算

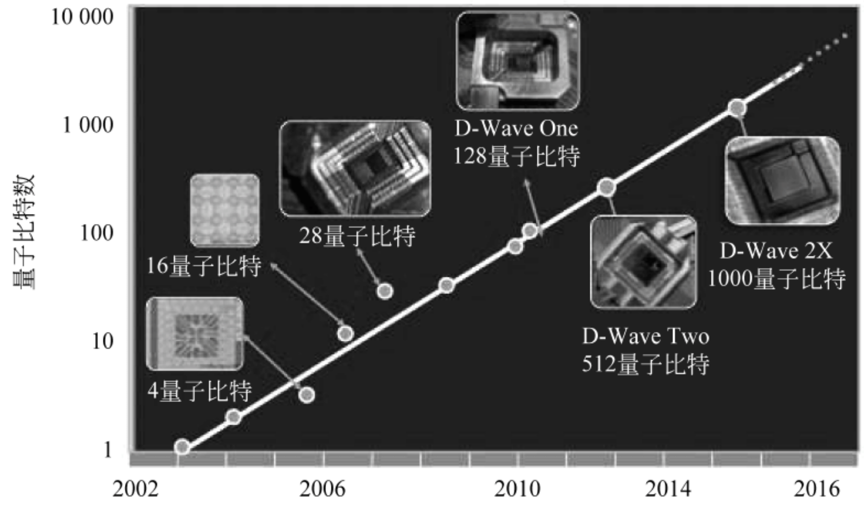


图 1-4　量子比特的发展

的开路先锋和标准制定者。量子计算机容量日益增加这个现象被称为罗斯定律(Rose Law)，该定律以 D-Wave 公司的首席技术官乔迪·罗斯(Geordie Rose)命名。

图 1-5　D-Wave Systems 公司位于加拿大温哥华的量子计算机

量子计算的罗斯定律就好比半导体处理器领域的摩尔定律。基本上，量子计算机的速度已经变得很快。

D-Wave 公司处于量子计算商业应用的最前沿，但是有一些细节需要考虑。D-Wave 公司还没有做出一款通用量子计算机。它好比是针对特定应用的处理器，经过了调优，旨在处理一项任务——解决离散优化问题。这对应于许多现实世界的应用领域，从金融、分

子建模到机器学习，不一而足，但是它不会改变人们目前的个人计算任务。

在短期内，假设它会应用于科学超级计算任务和商业优化任务，可能会隐藏于互联网巨头的数据中心，改善图像识别及其他形式的近似人工智能的神奇任务。在大多数情况下，量子计算机对经典计算集群而言将是起到加速作用的协处理器。

D-Wave 公司向谷歌之类的客户销售和出租量子计算机。据说这些机器的成本为1000～1500 万美元。

就算 D-Wave 机器在大众使用上还没普及，IBM 公司已经开始在提供“世界上第一个通过 IBM 云提供的量子计算平台”，旨在让公众可以发掘量子处理能力。

2017 年 11 月，IBM 公司公布了世界上第一台 50 量子比特的量子计算机。它诞生在一个实验室里，在一个巨大的白色箱子里，用泵保持它的最适宜温度，还有一些传统的计算机管理被启动的任务或算法。

这就是 50 量子比特的量子计算机样子！近距离观看，别具匠心，如图 1-6 所示。

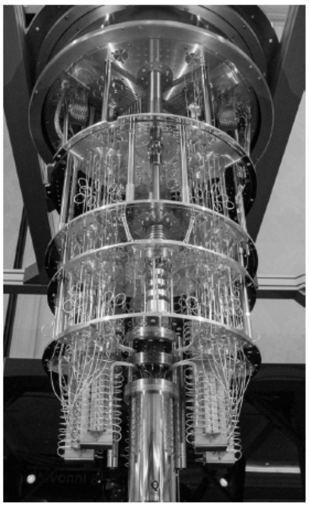


图 1-6　50 量子比特的量子计算机

在 2017 年的国际消费电子展上，IBM 公司带来了内部结构——需要将信号发送到芯片上的电线和管道，从而让系统保持适宜的超低温温度。从远处看，它就像是蒸汽朋克的枝形吊灯，或者是一系列错综复杂的管子和电线，最终达到底部的一个小钢瓶。

事实上，它是有史以来最复杂的量子计算机之一。处理器内部有 50 量子比特，它们以一种突破传统计算机的革命方式进行任务处理。通常，信息被创建并存储为一系列的 1 和 0。

量子比特可以同时表示两个值（被称为叠加），这意味着量子计算机可以同时对两者进行测试。添加更多的量子比特，这种计算能力会增加到令人难以置信的程度。

IBM 公司的研究人员介绍说，最大的挑战是将芯片从不需要的噪声中分离，包括电、

磁和热噪声。

1.23　量子计算将在我们有生之年普及

在科学技术领域，人们多年来一直对研发量子计算机充满热情，但它还尚未走进我们的日常生活。可是量子计算机从科学理论转向大众普及，也许并不需要30年那么长时间。很快我们会开始发现量子计算机能在更广泛的范围内发挥作用，包括物质科学、化学领域、物理系统、人工智能和机器学习等。量子系统可以无缝地加密数据，并帮助人们对已经收集到的大量数据进行理解分析，甚至能够解决即使是最强大的超级计算机也无法解决的复杂问题，如医疗诊断和天气预报。目前尚未成熟的量子技术正在变得更加接近人们想要的技术水准了。

量子计算机的核心是什么样的呢？

如果你走进一个带有量子机器的房间，你会看到一个真空室或导管，以及一束照射到它的激光，而且在本体里面有一个很低密度的特定的原子。人们使用激光减缓非常接近能量绝对值为零的原子运动，这就是激光冷却。目前，系统需要的环境温度大约需要接近绝对零度，系统需要保持适宜的超低温温度的部分如图1-7所示。

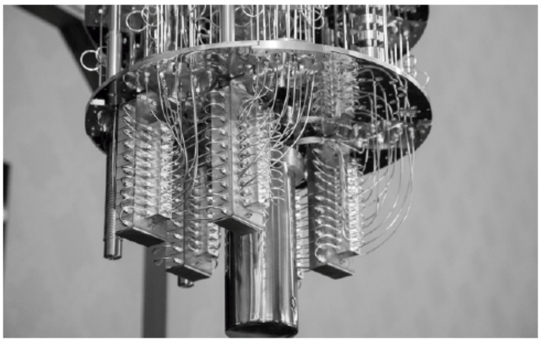


图1-7　系统需要保持适宜的超低温温度

量子计算机最有可能的应用是什么？

说实话，目前没有确定的答案。一般认为，量子计算机不一定会对所有的计算任务有帮助。即使是最好的传统计算机也有在数学问题上难以解决的时候。这就像假设你想给

一群人送一种礼物，而每个人都有自己感兴趣的东西，所以对于这个礼物来说，这些不同的兴趣点可能是矛盾的。

所以会发生的是，如果你用传统的方式解决这个问题，你必须对这群人每一对或三个一组进行检查，以确保至少他们的兴趣点是满意的。这个问题的复杂性非常迅速地增长，因为你需要检查的经典的组合数量是以指数计算的。这里有一些人相信，对于这类问题，量子计算机比传统计算机更有优势。

实际上，量子计算机的一个重要意义在于，我们已经建立了足够大、足够复杂、足够量的机器帮助我们进行科学实验，即使是世界上最好的传统计算机，例如超级计算机也不可能完成量子计算机进行的科学实验。

在实践中，量子计算机和传统计算机将可能携手合作。事实上，最可能的情况是，大部分主要的工作是由传统计算机完成的，但是其中一些最困难的问题，可以通过量子计算机解决。

另外，还有一个领域就是量子通信，它可以使量子态在站与站之间进行传输。而且，通过这些量子网络（有时也被称为量子互联网），人们能够远程访问量子服务器。这样，当然可以想象量子计算机可以进入日常生活的许多可能性，即使你不能把它放在自己的口袋里。

我们还不知道量子计算机将如何做到上面说的这些，但可以相信，很快就会知道的。

1.3　计算机和力学

1.3.1　量子力学与现实生活有什么联系

在日常生活中，人们常用到的是牛顿经典力学。但是随着人类对世界认知的不断进步，发现用经典力学不能完美地解释许多问题。例如黑体辐射的问题，光干涉实验中的明暗纹；再如紫外灾难，卢瑟福原子模型对电子轨道的描述存在矛盾等。正是这些东西让人们逐渐地接近这一对人类来说完全陌生的领域。

总体来说，量子力学是一套希望能描述这个世界不论是微观还是宏观所有物理规律

的理论。如今人类对量子理论的了解，除通过广义相对论描写的引力外，至今所有其他物理基本相互作用均可以在量子力学的框架内描写（量子场论）。

随着量子力学的完善，它在生活中的应用也越来越广。例如激光技术、电子显微镜、核技术，甚至会在不久的将来出现，以及现在已经取得一定进展的量子通信（绝对没有延迟的通信）、量子计算机（一个量子单位可以同时进行多种运算）等。

人类的眼光永远没有只着眼于现在，如果有朝一日人类将量子理论完善并应用于现实生活中，那么那个时代的人的生活将是我们今天的人完全无法想象的！可能就像古人与我们现代人的差距。

1.3.2　什么是量子力学

宏观世界的生活经验很多都是表象，例如你可能认为世界的运行是确定的、可预测的；一个物体不可能同时处于两个相互矛盾的状态。但是在微观世界中，这种表象被一种叫作量子力学的规律打破了。

量子力学指出，世界的运行并不确定，人们最多只能预测各种结果出现的概率，一个物体可以同时处于两个相互矛盾的状态中。量子计算是直接利用量子力学的现象（例如量子叠加态）操纵数据的过程。

1. 量子科技的基础是量子力学

量子力学是一个与牛顿力学等经典力学差异很大的物理学分支，由普朗克、爱因斯坦、德布罗意、玻尔、海森伯、薛定谔等物理学家创立。它是迄今为止描述微观世界最准确的理论，也堪称世界上最难理解的科学理论。玻尔有句名言：“如果谁不对量子论感到困惑，他就没有理解这个理论。”物理学家费曼则说：“我想我可以很确定地说，没有人理解量子力学。”

自从量子力学的创始人玻尔（也可以算上普朗克、海森伯、薛定谔、波恩等）在20世纪初建立氢原子模型以来，量子力学经历了约100年的风风雨雨，不过量子力学的“黄金时期”是在1920年至1929年这10年，说量子力学的“圣地”应该是哥本哈根、哥廷根、慕尼黑，这三个地方被誉为“黄金三角”。

量子力学的基本方法是海森伯的矩阵力学和薛定谔的波动方程，他们看似不同，但都是从不同的角度阐述微观世界的基本规律，一个偏向于粒子的角度，一个偏向于波动的角度，最后被证实它们是等价的。也就是说，世界的本质是波粒二象性！

其次，量子力学的基本原理有三个：波恩的概率解释、海森伯的不确定关系、玻尔的互补原理。

前两个原理共同摧毁了自牛顿以来的因果观。也就是说，在量子力学看来，一个结果可以被不同的原因引起，同一个条件也可以引起不同的结果，只不过是概率不同。因此，你不能说因为这个所以那个，而只能说这个可能引起那个。

玻尔的互补原理说：世界本身是粒子和波的和谐统一。不能说电子“到底是粒子还是波？”只能问“我这样观测，粒子会显示波动性还是粒子性？”也就是说，电子是什么，取决于观测手段，在微观世界，不存在绝对的客观存在，只存在可观测的物理量。

2.量子物理不同于经典物理的地方

下面是一些与你的问题不很相关，但也值得浏览一下的解说。

量子物理不同于经典物理的一个地方：量子物理认为量子系统在微观测之前可以处于客观的不确定状态（不是由于我们主观上尚不认识事物的那种主观不确定），观测可使量子系统“缩编”到某个确定的状态。

经典物理是没有“客观的不确定状态”一说的——它认为，即使人们不知道系统的确切状态，系统在客观上也是处于某个确定的状态。

这一重要区别，作者认为，更真实的量子系统一般总是处于多种状态共存的叠加状态（或说，多种状态都是潜在的、隐含的），一次测量，可使其中一种状态成为显现的状态……总之，多态叠加是量子力学的微妙的核心之一。

费曼说过：量子力学本身就是一个奥秘。其一是动量与波长关联，其二是振幅是复数。负动能意味着虚动量，这又使得描述实动量的振荡式的波动，变成了指数衰减函数，这意味着粒子可入负动能区，但概率要指数递减……这就是量子力学描述世界的方式，迥异于经典物理方式。

我们不能像经典物理要求的那样可以知道粒子在任意时刻的确切位置与速度，只能

从波函数得知其位置与速度的概率分布，而这种概率分布也是一种规律。

经典物理认为，粒子与波动是两个层次的东西，根本不是一回事儿；而量子力学却认为两者是相伴相随、密不可分的一个整体，是一体的两面，没有谁产生谁的问题。

3.造出量子计算机还需要目前不存在的物理学突破

在量子力学中，物质的状态虽然可以通过实验和计算确定，但是观察的结果却不是绝对的，每一次观察可能发现不同的结果。如果我们有能力复制很多个状态完全一致的物体，并对它们分别进行观测，如果都能得到相同结果，那么说明这个物体处在观测空间的某个本征态上。如果观测结果不同，那么说明该物体处在该空间一系列本征态的叠加状态上。

这些不同的结果，就是物质在一系列空间中本征态的叠加，称为叠加态。这种量子状态在宏观世界几乎是不可能观察到的，“薛定谔猫”这个思想实验可以帮助人们理解这种有点违反常识的现象。这个实验在后面有专门的章节解释。如同猫具有“又死又活”这个叠加态，在量子力学描述的世界中，虽然事件的因果是必然的，但是看到的结果却有可能是不同的。

量子力学描述了粒子的另外一种特性——自旋。这种特性无法用本征态表示，除了可以用 0 和 1 描述正向自旋和反向自旋之外，这两者之间还有多种不同的状态。最小单位称为量子比特。

如同电子计算机中的二进制位，量子比特是理论中量子计算机的计算基础。量子计算机对每一个叠加态分量实现的计算相当于进行一次传统的计算。所有这些传统计算同时完成并按一定的概率振幅叠加起来，即是量子计算机的输出结果。可以这么说：“不太准确的比方，传统电子计算机按时间顺序串行解决一个问题，理论上量子计算机就能解决同时并行 2^n 个问题。”

量子计算机可以对叠加态进行运算，但是运算结果本身也是叠加态。只有针对特定的问题，才能用特定的算法从叠加的结果中抽离出需要的信息。而且，遵循不确定性原理，任何对量子叠加态的测量都会导致波函数的坍缩，一旦坍缩就会出现一个确定的状态，量子叠加态消失，所有在叠加态基础上进行的计算都将不复存在。

也就是说，造出量子计算机还需要目前不存在的物理学突破。有个流传甚广的说法：“造出量子计算机的成功率与造出反重力汽车差不多。”

但是，“目前不存在的物理学突破”已经出现了，这就是全新的计算理论的出现，且看1.3.3节介绍。

1.3.3 全新的计算理论诞生

全新的计算理论诞生源于传统计算机搞不定的事情。

2010年，美国麻省理工学院(MIT)的计算机科学家提出在量子光学系统中，进行“玻色采样”的任务，但这一任务传统计算机不可能完成。因此，人们开始构想使用量子实验装置进行量子物理实验的模拟。实验的成功催生了一种全新的计算理论。

由于量子科学实验的技术解释需要比较深厚的量子物理学知识，所以，这里暂且进行粗浅的解释。玻色采样，就是 N 个光子跑进实验装置中，又随机从其中 N 个出口跑出来的过程。用传统计算机解决这个量子问题，采样的时间会非常长。如果一共有 N 个光子参与实验，传统计算机的采样时间，就会是呈 $N^2 \times 2^N$ 的规律增加，比直接做玻色采样实验慢得多。如果量子光学实验设计得合理，肯定比传统计算机的速度快。所以，这个实验装置本身，可以称之为一种光量子计算机，而它“计算”的内容，正是对输出光子的分布进行采样。

如果光子的数量达到50个，在传统计算机看来，计算量就会增加到 3×10^{18} 次。即使用目前的超级计算机，都不可能很快完成一次玻色采样，只能直接在装置上做实验。这就是一种“量子优越性”。

量子计算机的优势：当它有 N 量子比特时，由于状态相互叠加，它最多可以同时处理 2^N 个状态。不过，需要处理的量子比特越多，制造难度就越大。

1.4 10分钟看懂量子比特、量子计算和量子算法

宏观世界的生活经验很多都是表象。例如，你可能认为世界的运行是确定的、可预测的；一个物体不可能同时处于两个相互矛盾的状态。在微观世界中，这种表象被一种叫作

量子力学的规律打破了。

什么是量子？

前面已经讲过，量子是物理世界里最小的、不可分割的基本单元，是能量的最基本携带者。它是光子、质子、中子、电子、介子等基本粒子的统称。可以说，整个世界都是由量子组成的。例如，日常生活中的光，就由大量光量子组成。

量子力学指出，世界的运行并不确定，人们最多只能预测各种结果出现的概率；一个物体可以同时处于两个相互矛盾的状态中。

量子计算，就是直接利用量子力学的现象（例如量子叠加态）操纵数据的过程。下面简单地介绍什么是量子、量子叠加态、量子比特、量子测量和一种实现随机数据库搜索的量子算法。

量子有不同于宏观物理世界的奇妙现象，例如波粒二象性，还有最为著名的量子叠加和量子纠缠。

1.4.1　波粒二象性

波粒二象性（Wave-particle duality）是量子粒子的特征，它是指微观粒子基于不同的环境，有时会表现出波动性，而有时表现出粒子性。

微观世界的奇异性在于“波粒二象性”，即微粒不再像以往以为的那样，是个小小的实体球一样的东西，而且可以沿着一条确定的轨迹运动。它实际上已没有什么确切的大小、形状、位置、轨迹可言，这些经典概念统统不适于描述微观世界及其运动。微粒已变得像波那样弥散于广阔的空间里。所有微粒都具有波粒二象性——它既像颗粒状分离的粒子，又像云雾状弥散的波动，而且粒子的动量直接与波动的波长成反比。

例如光就具有粒子和波的双重性质，图解如图 1-8 所示。

量子理论的特点是找到给定点 x 在空间中存在的概率，而不是它的确切位置。

1.4.2　量子纠缠

量子纠缠指的是量子粒子之间的相互作用。即使粒子间相隔甚远，它们依然相互作

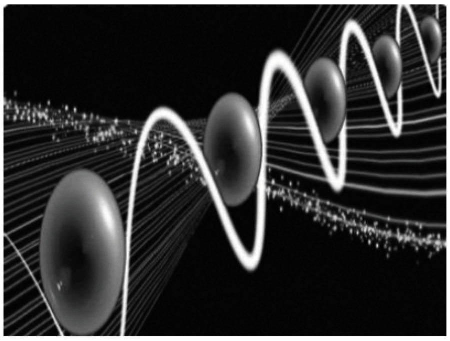


图 1-8　光具有粒子和波的双重性质

用、相互参照，而不是独立的。

量子纠缠也是量子叠加的一种表现，两个处在纠缠态的量子一旦分开，不论分开多远，如果对其中的一个粒子测量，另一个粒子就会立即发生变化，且是不需要时间的变化。

为了说明这个复杂的问题再举个例子：你工作需要去上海出差了，你太太怀孕10个月被送进北京协和医院妇产科，突然肚子疼，被送进产房，30分钟后你的儿子出生了。那又怎么样呢？在你儿子诞生的那一刹那，你在北京的太太成了妈妈，在上海的你成了爸爸！这是不是可以增加你对“纠缠”一词的理解，不知道我说清楚了没有？

这两个纠缠在一起的量子就好比是一对有心电感应的双胞胎，不论两人距离多远，千米量级或者更远，只要当其中一个人的状态发生变化时，另一个人的状态也会跟着发生一样的变化。爱因斯坦称之为“幽灵般的超距作用”。量子纠缠所体现的这种非定域性是量子力学最神奇的现象之一。

在测量时，如果一对纠缠的量子被决定处于箭头向下↓的自旋态（能量最低状态），则当电子与它的磁场保持一致时，这个状态就会被传递到另一个相关的箭头向上↑的相对自旋态的粒子上。量子纠缠允许相隔很远的量子比特彼此之间及时相互作用。

1.4.3　量子叠加

量子同时以0和1的形式存在，这种现象被称为叠加。

虽然粒子能存在于多个量子态中，一旦确定了粒子的能量或位置，叠加至此消失，它

只能存在一个状态。

量子世界跟宏观世界最大的区别，就是量子有多个可能状态的叠加态。这种现象在宏观世界中不存在且也无法维持。在宏观的经典世界中，1 就是 1，2 就是 2。而在微观的量子世界中，一个状态可以存在于 1 和 2 之间，它既不是 1，也不是 2，但它既是 1，又是 2。

这说起来有点悬，历史上世界最著名的几个科学家也吵了若干年，我们后面有足够的章节讲这个事情。先打个比方，这就好比孙悟空的分身术。一个孙悟空可以同时出现在多个地方，孙悟空的各个分身就像是他的叠加态。在日常生活中，一个人不可能同时出现在两个地方。但在量子世界里，作为一个微观的客体，它能够同时出现在许多地方。

下面就一些比较复杂的概念进行解释，先大概描述一下粗浅的含义，以后的章节再进一步详细地解释。

1. 量子叠加态

下面需要解释一下量子叠加态。

夏天到了，烈日炎炎。当你带上偏振墨镜时，从某种程度上讲，你就已开始接触量子计算了。偏振墨镜就是我们了解量子叠加态的起始案例。

为什么这么说呢？因为光的偏振正好“同时处于两个相互矛盾的状态”中，也就是量子叠加态。在量子计算中，光子的偏振就可以用来实现量子比特。

首先，光是一种电磁波，组成它的粒子叫作光子。电磁波的振动就像绳子抖动一样，可以朝这儿偏也可以朝那儿偏，形成各种各样的偏振。

其次，偏振墨镜就像一个筛子，只有跟筛子的缝隙方向一致，光子才能“钻过去”。如果跟筛子的缝隙方向垂直，光子就被完全“拦住”了。

如果光子偏振方向跟缝隙方向既不垂直也不平行，而是呈一定角度，又会怎样呢？

如果你在钻过去的朝↗方向偏振的光子后面，再放一个只过滤↑光子的偏振镜，就会发现一个非常诡异的量子力学现象：大约有一半儿↗偏振光子穿过了偏振镜，而且偏振方向都变成了↑。这真是一个非常诡异的量子力学现象。

这个时候，运用高中学过的矢量合成知识，我们可以试着解释这个现象。由于光子的偏振既有方向又有大小，我们可以将每个光子的偏振看作一个矢量。于是，它们满足矢量

的加法。

由于↗方向的振动等于↑方向的振动加上→方向的振动，我们就可以说，↗偏振的光子可以看作是同时在朝↑和→方向振动。矢量既有长度又有方向，这时就是其矢量的相加（见图 1-9）。

矢量↗可以看作矢量↑加上矢量→：$\boldsymbol{C}=\boldsymbol{A}+\boldsymbol{B}$。

而光子同时在进行两种振动的情况可以解释如下：一种振动可以看作由两种不同的振动相加而成，所以，光子可以看作是同时进行两种振动，即↗偏振的光子可以看作它同时进行的↑振动和→振动的合成。

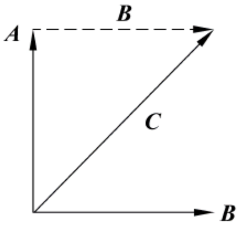


图 1-9　矢量相加

如果你不理解什么叫同时进行两种振动，想想你耳朵里的鼓膜，正是它同时进行多种振动，你才能同时听到各种各样的声音。

这时，我们就可以试着解释那个奇怪的量子现象了。如果把一个↗偏振的光子看作是一个光子同时进行↑和→两种振动，那么可以说，当这个光子路过↑偏振镜时，其中一半儿→振动被挡住了，另一半儿↑振动通过了。

2. 量子态测量的概率性

然而，这个上面的解释并不完全正确。

如果朝这个偏振镜发出一个↗光子，在偏振镜之后，并不会接收到一个振动能量减弱一半儿的光子，而是有 50％的概率接收到一个↑光子；50％的概率什么也没接收到。也就是说，当你测量一个量子叠加态时，总会得到概率性的结果。记住量子测量的概率性，这在后面的量子算法中会用到。

到这里你可能想起来了，这就是量子力学常说的“上帝掷骰子”。根据不同的偏振方向，得到的概率也是不同的，如图 1-10 所示。

注解：虽然↗方向的光子处于两种振动的叠加状态，但当你通过↑偏振镜测量它时，它总会随机地“掷骰子”，以一定概率得到↑方向或→方向的结果。“掷骰子”的概率与偏振方向的夹角有关。偏振方向跟↑方向的夹角有关。偏振方向跟↑方向的夹角越小，测量时得到↑偏振的光子的概率就越大。偏振方向与→方向的夹角也是同理。

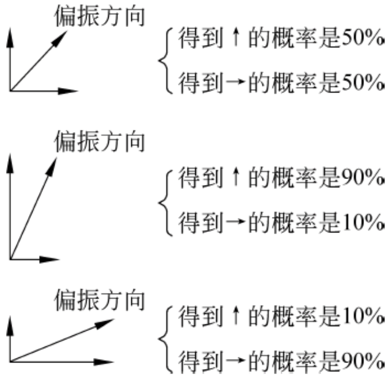

偏振方向
得到↑的概率是50%
得到→的概率是50%
偏振方向
得到↑的概率是90%
得到→的概率是10%
偏振方向
得到↑的概率是10%
得到→的概率是90%

图 1-10 不同偏振方向得到的概率不同

1.4.4 量子比特和量子计算

1. 量子比特

如果把↑光子看作比特 0，把→光子看作比特 1，那么，一个↗光子就处于比特 0 和比特 1 光子的叠加状态之中。

如果硬要用一个偏振镜去测量它到底是比特 0 还是比特 1，就会发现，测量结果有 50％的概率是比特 0，还有 50％的概率是比特 1。

↗光子所携带的这种诡异的“比特”就叫作量子比特。可以把比特 0 和比特 1 分别想象成一个虚拟的空间中的两个相互垂直的坐标轴。对于经典比特来说，它要么处于比特 0 的轴上，要么处于比特 1 的轴上。

而量子比特可以在两个轴之间的空间任意“转动”，量子比特在两个轴之间的空间任意“转动”的结果，以一定比例得到比特 0，一定比例得到比特 1。

2. 量子计算

1）量子门

电子计算机所做的计算，就是操纵经典比特。

同样的道理，所谓量子计算机，就是在量子力学允许的范围内操纵量子比特。这时就需要可以操纵电子比特的量子门。

量子逻辑门是一个对特定的量子比特在一段时间间隔实现逻辑变换的量子逻辑线路，它是量子线路的基础。与传统逻辑门不同，量子逻辑门是可逆的。

量子逻辑门是量子计算与量子计算机实现的基础，可用下列方法实现。

（1）量子点系统。

（2）超导约瑟夫森（Josephson）结系统。

（3）核磁共振量子系统。

（4）离子阱系统。

（5）腔量子电动力学系统等。

量子逻辑门按照其作用的量子比特的数目可分为单比特门、二比特门和三比特门等。

2）量子并行计算

不知道你发现了没有，由于量子比特可以同时处于比特 0 和比特 1 的状态，量子门操纵它时，实际上同时操纵了其中的比特 0 和比特 1 的状态。

所以，操纵一量子比特的量子计算机可以同时操纵 2 个状态。如果一个量子计算机可以同时操纵 N 量子比特，那么它实际上可以同时操纵 2^N 个状态，其中每个状态都是一个 N 位的经典比特。这就是量子计算机传说中的并行计算能力。

3）量子计算机算法

1985 年，英国牛津大学 Deutsch 研究了量子图灵（Turing）机，引进了量子计算线路模型和量子通用逻辑门组，突破了经典计算布尔（Boole）逻辑的限制，实现了到量子演化的跃进。在那之后，科学家们开始了对量子算法的研究。

（1）Shor 算法。

Shor 算法是由美国贝尔实验室的科学家彼得·秀尔（Peter Shor）在 1994 年提出的分解大数质因子的量子方法。互联网时代绝大多数的加密，都由 RSA 算法完成，目前支付宝、微信支付、微众银行等都在采用 RSA 2048 加密算法，但随着量子计算的发展，RSA 加密安全性受到了挑战。例如，Shor 分解大数质因子时，传统计算机与量子计算机使用的时间和硬件环境如表 1-1 所示。

表 1-1　Shor 分解大数质因子的量子方法比较

分解一个2048位的数	传统计算机	量子计算机
时间	10 年	24 小时
硬件	占据 1/4 北美面积的服务器农场	小房间里的一台量子计算机，内含 100 万量子比特

（2）Grover 算法。

Grover 算法是由 Grover 于 1996 年提出的平方根加速的随机数据库量子搜索算法。搜索算法常用于从 N 个未分类的记录中找出某个特定的记录。

Grover 量子搜索算法可以对随机数据库相对经典搜索平方根加速，为了实现这样的加速，Grover 算法主要依赖于量子态的叠加。

假设有 N 个未经排序的数据。如果使用经典算法寻找其中的某个数据 x，条件是它（并且只有它）满足 $P(x)=\text{TRUE}$，比方说 x 代表一个人的工号，$P(x)$是看这个人是不是现任 CEO。那么你只能从第一个数据开始，一个一个地看它是不是 CEO 的工号。使用经典算法寻找其中的某个数据 x 的方法是：对于未经排序的数据，经典的算法只能一个一个地找，运气最差的时候你得计算 N 次才能找到那个数据。

在这种算法中，计算复杂度是 $O(N)$。

在 Grover 算法中，可以将 N 个数据同时存储在 $\log_2 N$ 量子比特中，然后同时计算 N 个函数 $P()$的取值，就相当于同时在 N 个状态上做了 N 次 $P()$的计算，也就是同时看它是不是 CEO 的工号。

在 N 个计算结果中，必然有一个结果是 CEO 的工号，其他结果都不是。但如果这个时候贸然去“读取”结果就会发现，每个结果发生的概率都是 $1/N$。这就好比你用↑偏振镜去测量↗光子，得到↑和→的概率各为 1/2。

Grover 算法的思想是，同时计算 N 个 $P()$的取值后，先不要读取，而是通过量子操作略微增加结果为 CEO 工号的那个数据发生的概率。

数学计算证明，反复重复以上过程$(\pi\sqrt{N})/4$ 次之后，你要找的那个数据发生的概率就会达到最大。这个时候如果再去读取数据，就会以极大的概率读到你要找的数据。

所以，Grover 的量子搜索加速算法，可以将搜索复杂度降低到 $O(\sqrt{N})$，但你成功读取那个数据的概率永远也不会达到 100%，而是略小于 100%。

从目前的情况看，量子计算只是在少数计算任务中表现得比经典计算更快，例如大数质因子（Shor 算法）、随机数据库搜索（Grover 算法），并且，这种快法不能挣脱量子力学的约束，达到十全十美。

1.5 量子计算机是什么计算机

1.5.1 什么是量子计算机

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息，运行的是量子算法时，它就是量子计算机。

1. 量子计算机的提出

量子计算机的概念源于对可逆计算机的研究，研究可逆计算机的目的是为了解决计算机中的能耗问题。研究发现，能耗来源于计算过程中的不可逆操作。那么，是否计算过程必须用不可逆操作才能完成呢？问题的答案是所有经典计算机都可以找到一种对应的可逆计算机，而且不影响运算能力。

由此，科学家想到既然计算机中的每一步操作都可以改造为可逆操作，那么在量子力学中，它就可以用一个幺正变换表示，从而运用到量子计算机中。幺正矩阵是基本的物理概念，是指如果一个 n 阶方阵，它的列向量构成一组标准正交基，那么这个矩阵就是幺正矩阵。由幺正矩阵所表示的变换称为幺正变换。

当今的计算机厂商提供的强大计算处理能力仍不能满足人们对运算速度和运算能力的渴求。1947 年，美国计算机工程师霍华德·艾肯（Howard Aiken）曾说，只要 6 台电子数字计算机就可以满足全美国的计算需要。

现在，是不是还有什么大腕说有多少台量子计算机就可以满足全世界的需要了呢？

据调查，还没有人说出这样的话。

2. 集成电路的发展极限

人们现在使用的大规模集成电路是有极限的。早在20世纪，1990年已经制成了64M位的动态随机存储器，集成电路的线宽已细到0.3μm。1993年制成了256M位的动态随机存储器。当存储器达到1024M位时，集成电路的线宽将细到0.1μm，也就是千万分之一米，差不多是一根头发丝的千分之一。这样细的电路，被认为是集成电路的发展极限，电路比这更细时，现有电子元件将失去工作的理论基础。

实际上，早在1981年，美国物理学家理查德·费曼(见图1-11)已提出，人们能够研制出“遵循量子力学法则的微型计算机”。他认为，这样的量子计算机可能是模拟现实世界量子系统的最好方式。

费曼是美国著名的物理学家，1965年度诺贝尔物理学奖得主。他提出了费曼图、费曼规则和重正化计算方法，是研究量子电动力学和粒子物理学不可缺少的工具。

自那时起，各国科学家一直在研制量子计算机，但结果始终不尽如人意。早期的量子计算机，实际上是用量子力学语言描述的经典计算机，并没有用到量子力学的本质特性，如量子态的叠加性和相干性。

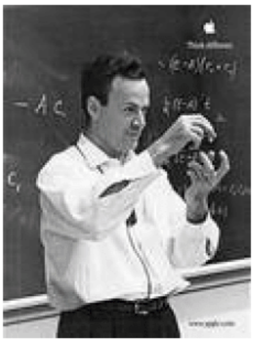


图1-11　美国物理学家理查德·费曼

1.5.2　量子计算机的前世今生

1. 量子计算机的前世

1920年，薛定谔、爱因斯坦、海森伯和狄拉克，共同创建了一个前所未有的新学科——量子力学。量子力学的诞生为人类未来的第四次工业革命打下了基础。在此基础上人们发现了一项新技术，就是量子计算机。

量子计算机的技术概念最早由费曼提出，之后经过很多年的研究这一技术已初步见成效。在20世纪80年代多处于理论推导等纸上谈兵状态。一直到1994年秀尔提出量子质因子分解算法后，因其对于现在通行于银行及网络等处的RSA加密算法可以破解而

构成威胁之后，量子计算机变成了热门的话题。除了理论之外，也有不少学者着力于利用各种量子系统实现量子计算机。

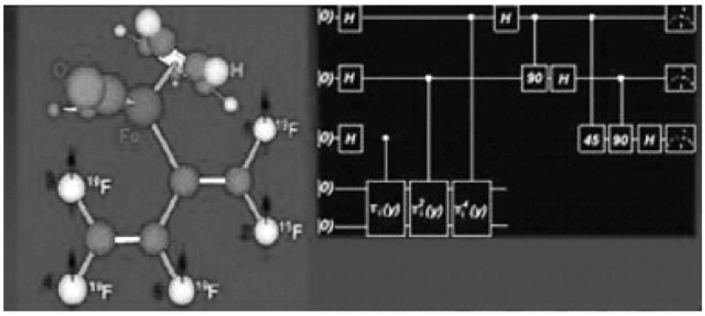
2.现代量子计算机的今生

1994年，两位物理学家尼尔和艾萨克研制出一台最基本的量子计算机，能够进行简单的运算。使用丙氨酸，它可以完成1+1的运算；使用液态三氯甲烷，还能解决其他问题。物理学家们现在正努力研究出一种比较复杂的计算机，能够将15分解成3乘5。

2000年，日本日立公司开发成功一种量子元件——单个电子晶体管，可以控制单个电子的运动，具有体积小、功耗低的特点，约是目前功耗最小的晶体管的千分之一。日本富士通公司正在开发量子元件超高密度存储器，在1cm^2芯片上，可存储10万亿比特的信息，相当于可存储6000亿个汉字。美国物理学家约翰逊开发成功的电子自旋晶体管，有可能将集成电路的线宽降至0.01μm。在一个小小的芯片上可容纳数万亿个晶体管，使集成电路的集成度大大提高。

2000年3月，美国洛斯阿拉莫斯国家实验室的科学家们宣布研制了一台包含7量子比特，存在于一滴液体中的量子计算机，如图1-12所示。该量子计算机使用核磁共振操纵反式丁烯酸分子原子核中的粒子。反式丁烯酸是一种简单的液体，其分子由6个氢原子和4个碳原子组成。核磁共振可用来产生促使粒子排列起来的电磁脉冲。处于与磁场方向相同或相反位置的粒子，使得该量子计算机可以模仿数字计算机按比特对信息进行编码。

5量子比特215Hz量子处理器



分子结构　　　　量子线路

图1-12　存在于一滴液体中的量子计算机

2000年8月，IBM Research-Almaden研究中心宣布制成了一台据称是当时最先进的量子计算机。这台量子计算机的5量子比特由5个相互作用的氟原子核构成，使用无线电频率脉冲编程，并使用类似于医院中的核磁共振（NMR）设备（有关详细信息可参见核磁共振成像原理）进行探测。这支由艾萨克·庄（Isaac Chuang）博士领导的IBM小组成功地仅用一步解决了一个用传统机器需要循环才能解决的数学问题。这个称为寻秩的问题涉及查找一个特定函数的周期，是密码学中经常遇到的众多数学问题之一。

近年来由于社会对高速、保密、大容量的通信及计算的需求，促进了量子信息、量子计算理论与实验的迅速发展。目前，美国的洛斯阿拉莫斯国家实验室和麻省理工学院、IBM公司和斯坦福大学、中国科学院武汉物理研究所、清华大学的四个研究组已实现7量子比特量子算法演示。

2007年2月26日，加拿大一家公司宣布已经制造出了世界上首个商业量子计算机。

2007年年初，中国科技大学潘建伟小组在*Nature*·*Physical*上发表论文，成功制备了国际上纠缠光子数最多的“薛定谔猫”态和单向量子计算机，刷新了光子纠缠和量子计算领域的两项世界纪录，成果被欧洲物理学会和*Nature*杂志等广泛报道。

特别引人注目的是，英国*New Scientist*杂志在“中国崛起”的专栏中，把中国科技大学在量子计算领域取得的一系列成就作为中国科技崛起的重要代表性成果，进行了专门介绍。

1.5.3　量子计算机进入世界级竞赛

进入21世纪以来，量子计算机进入世界级竞赛。

相比传统计算机，量子计算机的最大区别在于：传统计算机只能按照时间顺序一个个地解决问题，而量子计算机却可以同时解决多个问题。

传统计算机使用的运算规则是二进制，用0和1记录信息状态。但量子计算机由量子状态描述信息，根据量子的特性，它可以同时表示多种状态，并同时进行叠加运算，因而拥有更快速的运算方式。

由于量子计算机的处理能力比当前传统超级计算机高几个数量级。因此，许多人认

为，量子计算机将完成以前被认为是不可能完成的任务，例如模拟化学催化剂、建立超级复杂系统的模型、破解加密密码等。但迄今为止，这些公司开发的量子计算机处理能力不够强大或不够精确，在运行大多数任务时不足以超过传统计算机。

量子计算机成熟商用时点逐步临近，超强运算能力对传统加密手段形成巨大冲击，量子通信绝对安全的理论特性愈加重要，量子通信的应用和推广有望进一步提速。传统计算机15万年才能完成的300位大数分解，量子计算机利用Shor算法只需1s，经典非对称密码体系全部能够被量子Shor算法破解。

目前，IBM、Intel公司均已推出17量子比特量子计算机，50量子比特产品商用也有望近期落地。量子计算机面世后，信息安全将无法保证，量子通信绝对安全的理论特点在量子计算时代格外重要，量子通信的应用和推广有望进一步提速。

1. IBM公司发布了17量子比特的处理器

2017年5月，IBM公司发布了17量子比特的处理器，如图1-13所示。其强大的计算能力，使得它可以应用于那些需要强大计算性能的场景，传统计算机是没法胜任这类工作的。量子计算机利用量子现象同时表示多个数据，这使得以往只能进行一次运算的时间内可以实现并行的复杂运算。

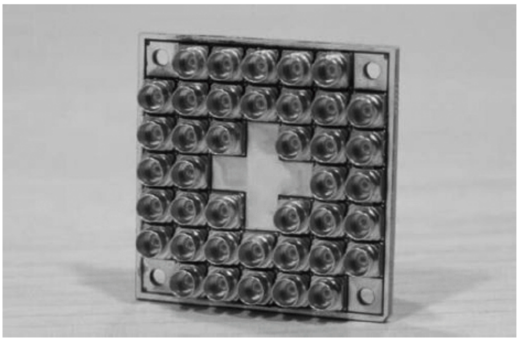


图1-13　17量子比特计算测试芯片

2. Intel公司交付49量子比特测试芯片：算力等于5000颗8代i7

Intel公司也在研究量子处理器，并在2017年10月携手荷兰研发合作伙伴QuTech量子实验室成功利用先进材料技术和制造技术开发出了一款包含17量子比特的新超导

芯片，并将芯片交 QuTech 进行测试，挑战 IBM 公司此前推出的规模最大的量子计算芯片。

目前，各大科技公司的研究员都在开发包含 50 量子比特的芯片。这样的芯片计算能力将超过当前所有超级计算机。

根据 Intel 公司介绍，量子计算的构建模块（也就是量子比特）相当脆弱，只能在极低温度下运行，而且封装时要求很高，必须预防数据丢失。Intel 公司找到一种新方法，它们制造出 17 量子比特芯片，芯片的架构在更高温度下更可靠，量子比特之间的射频干扰更小。

2017 年，Intel 公司已经成功设计、制造和交付 49 量子比特的超导测试芯片，这距离 Intel 公司交付 17 量子比特芯片仅仅过去了 3 个月的时间。

49 量子比特的芯片代号是 Tangle Lake，被 Intel 公司认为是里程碑。因为在这样的尺度上，已经允许研究人员评估改善误差修正技术和模拟计算问题。谈到量子计算的商用，还需要 5～7 年时间。

7、17、49 量子比特芯片如图 1-14 所示。

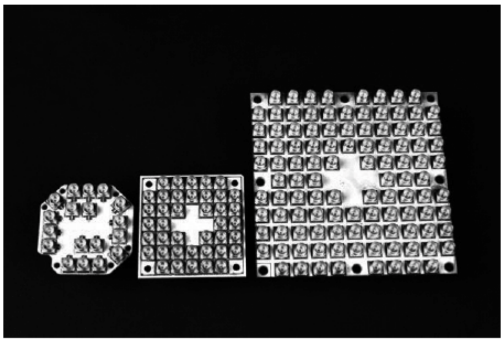


图 1-14　7、17、49 量子比特芯片

除了超导量子比特，Intel 公司也基于 300mm 制程工艺打造了 1 量子比特的自旋芯片。自旋量子比特的规模和单位面积比超导量子比特更可观，而且，它就像一个单电子晶体管。

3. Google公司宣布开源量子计算软件 OpenFermion

另一巨头 Google 公司也不甘示弱，它在自己的官方博客上宣布公开开源量子计算软件 OpenFermion，让科学家们更方便地使用量子计算机。这次开放的是 OpenFermion 的源代码，可供用户免费使用，化学家和材料学家可以利用 OpenFermion 改编算法和方程，使之能在量子计算机上运行。

Google 公司开源的做法也是量子计算机领域目前的趋势。IBM、Intel、Microsoft 和 D-Wave 等公司都曾宣布开放自己的量子计算平台，使之能促进量子计算的商业化运行。

4. 加拿大量子计算公司 D-Wave 发布全球第一款商用量子计算机

2017 年 D-Wave 公司宣布，推出旗下最新型号的量子计算机 D-Wave 2000Q，如图 1-15 所示。D-Wave 2000Q 的计算能力是以前型号的两倍，Temporal 防御系统公司是这台新计算机的首个客户，其主要目的是把 D-Wave 2000Q 用于网络安全研究。

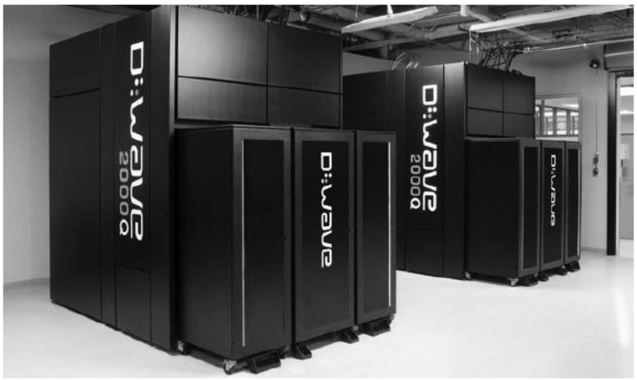


图 1-15　量子计算机 D-Wave 2000Q

在这之前，Google 公司购买了一台 D-Wave 量子计算机用来研究人工智能，美国国家宇航局 NASA 和军火商洛克希德·马丁公司也采购了同样的机型用于研究。

5. 美国 IBM公司成功构建 50量子比特原型机

IBM 公司从 2017 年开始以云计算服务的形式提供量子计算能力。IBM 公司宣布，已经成功开发了包含 50 量子比特的原型产品，量子计算机中的芯片所处环境温度被降至 15K，如图 1-16 所示。这是量子计算领域的下一个里程碑。IBM 公司最初版本的量子计

算机是免费提供的，目的是培育用户社区，指导用户如何使用这些机器编程。

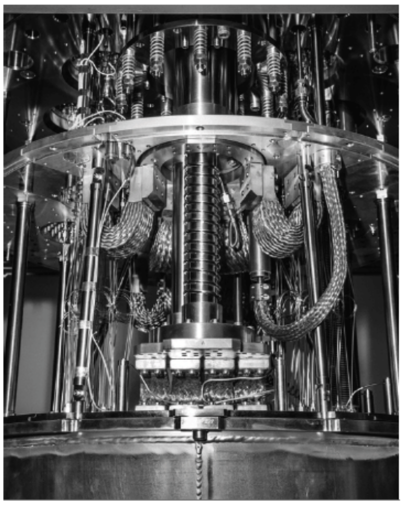


图 1-16　IBM 公司量子计算机中的芯片所处环境已降至 15K

量子计算机和量子信息技术在科技界的领先地位是不可动摇的。未来处理能力超强的量子计算机能够在数秒内完成目前速度最快的超级计算机数年才能完成的计算任务。可能未来的某天，你会发现现代的数字计算机已经因为过时而被丢进了历史的垃圾堆。量子计算虽然起源于理论物理这个高度特殊的领域，但是它的未来无疑有着深远的意义，它必将对全人类的生活产生深刻的影响。

6. Google 公司发布全球首个 72 量子比特通用量子计算机

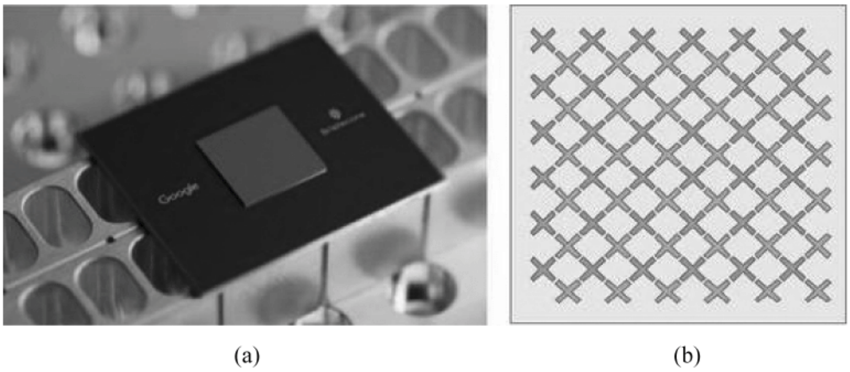
2018 年 3 月，Google 公司宣布推出一款 72 量子比特的量子处理器 Bristlecone，实现了 1％的低错误率，与 9 量子比特的量子计算机持平。

Google 公司认为，使用 Bristlecone 可以实现量子霸权。同时 IBM 公司也曝光了其 50 量子比特量子原型机内部构造。Google 公司在量子比特位数和错误率上的亮眼表现，霎时将 2018 年的量子霸权竞赛的赛点提前。这个最新设备遵循 Google 公司之前提出的 9 量子比特量子计算机的线性阵列技术所对应的物理学原理，而该技术显示的最佳结果如下：低的读数错误率（1％）、单量子比特门（0.1％）以及最重要的双量子比特门（0.6％）。该设备使用与 9 个量子比特的相同的模式进行耦合、控制和读出，但将其扩展

为一个包含72量子比特的正方形数组。

图1-17(a)是Google公司最新的72量子比特量子处理器Bristlecone。

图1-17(b)是该设备的图示：每个“×”代表一个量子比特，量子比特之间以线性阵列方式相连。



(a)　(b)

图1-17　Google公司最新的72量子比特的量子处理器Bristlecone

一直以来，大家都认为50量子比特的量子计算机是实现量子霸权的“起步价”。就在Google公司抛出49量子比特的量子计算机实现量子霸权的说法后不久，IBM公司就称，它们的研究表明，对于某些特定的量子应用，可能需要56个乃至更多个量子比特才能实现量子霸权。这可能是为什么Google公司从2017年的49量子比特一下子跳跃到72量子比特的一个原因，超出这么多，应该能打消各种疑虑。但是，要实现量子霸权，就不得不说刚才提到的量子模拟。目前最强大的超级计算机，只能模拟46量子比特。

7. 抢占2018年量子霸权竞赛赛点，小型商用量子计算机5年内出现

当我们可以实现几十乃至几百万量子比特0.1%～1%的错误率时，量子计算机将开始真正高效解决实际问题。这可能需要十年或者更久的时间。但是，至少Google公司认为，在制造出大规模量子比特量子计算机之前，我们可能会先实现一些小型的甚至是商用的量子计算机，或者说量子计算商业应用。2017年，Google公司量子团队在*Nature*刊文称，他们坚信即使还缺乏能够完整纠错的理论，但5年之内仍会有与量子计算有关的小型设备问世，而这也将给投资者带来短期的回报。早期的量子计算设备将在量子模拟、量子

辅助优化和量子采样领域有商业运用。更快的计算速度对从人工智能到金融和医疗等领域具有明显的商业优势。

1.6　未来世界是量子互联网的时代

预计2030年前，量子计算机将投入实际应用，解决许多具有重大经济和社会价值的问题。

1. 量子通信“无条件安全”

2016年8月，中国发射了世界上首颗量子科学实验卫星，并已建成量子通信“京沪干线”，在全球处于领跑地位。据预测，到2030年，量子通信将实现大规模应用。经典通信的硬件设施不会被取代，只需在原有设施上“锦上添花”——在通信发送端和接收端安装单光子探测器、量子网关等量子加密设备，即可在电话、传真、光纤网络等原有通信网络中实现量子通信，安全性大幅提升。中国正在构建的天地一体化量子通信网络如图1-18所示。

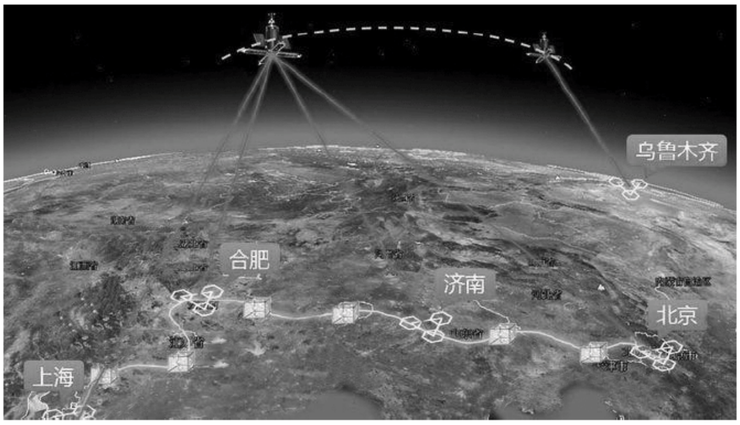


图1-18　中国正在构建的天地一体化量子通信网络

与经典通信不同，量子通信可以将信息编码，加载到单个光子的量子叠加态的偏振方向上。单光子是光能量的最小组成单元，不能被再分割，量子状态无法被精确复制，任何

窃听行为都会对其造成扰动，从而被通信双方察觉并规避。通过量子态传输，通信双方协商生成量子密钥，再加上对信息进行“一次一密”的加密保护，真正实现信息在传输中的完全随机、不可破译，从根本上解决通信安全问题。

2. 量子计算机将“秒杀”超算

利用 0+1、0－1 等量子叠加态，各国科技人员还在研发量子计算机。随着可操纵的量子数量增加，量子计算机的计算能力会指数级上升。

指数级上升的威力有多大？印度的棋盘麦粒故事很能说明问题。舍罕王打算奖赏国际象棋的发明人——宰相达依尔，就问他想要什么。达依尔对国王说：“请您在这张棋盘的第一个小格里，赏给我 1 粒麦粒，在第二个小格里给 2 粒，第三个小格里给 4 粒，以后每一小格中的数量都比前一小格加 1 倍。请您把摆满棋盘上所有 64 格的麦粒，都赏给我吧！”国王觉得这个要求太容易满足了，就命令手下搬来几袋麦粒。当记数开始一段时间后，国王才发现：就算把全世界的麦粒都拿来，也填不满这些象棋格子。

同样道理，当量子计算机可操纵的量子数达到一定级别，它的计算能力将会十分惊人。当计算机发展到 50 量子比特的时候，就能够实现“量子称霸”，对特定问题的处理能力远超现在的超级计算机。这意味着，许多大规模计算难题能得到有效的解决方案，在密码破解、气象预报、药物设计、金融分析、石油勘探等领域具有巨大的应用前景。

3. 中国量子通信技术领跑全球，未来十年拟构建量子互联网

最开始，人类结绳记事；然后，人们用语言和文字沟通；再后来，手机、网络成为必需品。信息传输，早已从如何传输，走入了“如何安全传输”的年代。

中国首颗“量子科学实验卫星”的发射成功，有望让量子通信真正进入广域传输时代；其“测不准”“不可复制”等特性，使得其传输的信息在理论上永不会被解密。

不过，发射卫星只是一个起点，在“宏伟量子大厦”中，量子“京沪干线”正在飞速搭建，天地一体的广域量子网络指日可待，市场应用不断突破。在第二次“量子革命”中，中国正在领跑。十年磨剑，量子通信从“三点一线”走到“洲际传播”。

目前，中国工商银行、北京农商银行等多家银行率先试用了量子通信加密技术。从理论上讲，通过设备产生量子密钥，再对数据进行加密传输，是不会被窃取的，这对金融数据

传输是非常必要的。

量子“京沪干线”总长2000多千米，建成后，目标应用于军事、金融、政务等领域信息的安全传输。金融机构、媒体、大型企业，都可以成为量子通信的用户。

4. 竞争加剧，“第二次量子革命”出现

量子信息技术方兴未艾，这一领域的国际竞争也在不断加剧。2017年以来，欧美纷纷提出“第二次量子革命”计划，加大基础研究和产业发展方面的投入。

2017年3月，欧盟委员会发布《量子宣言（草案）》，计划于2018年启动10亿欧元的量子技术项目。其中，在量子通信方面，规划5年内突破量子中继器核心技术，实现点对点安全量子通信。10年内实现远距离量子网络、量子信用卡应用等，目标是融合量子通信与经典通信，保卫欧洲互联网安全。美国更是将“量子跃迁”作为“六大科研前沿”之一，认为人类正站在下一代量子革命的门槛上，量子力学正在导致变革性技术，必须加大投入促进交叉性基础研究。

2017年5月在荷兰阿姆斯特丹举行了欧洲量子会议，这次会议上有参会者明确提出，欧洲要成为世界量子技术发展竞争中的领导者，并提议建设类似于中国量子通信“京沪干线”的项目。

发射全球第一颗量子通信卫星，无疑确立了中国在国际量子通信研究中的领跑地位。根据中国量子通信发展规划，量子卫星发射及建成量子通信“京沪干线”后，国内初步形成广域量子通信体系。到2030年左右，中国率先建成全球化量子通信网络。

1.7　现在最火的是量子通信

1.7.1　量子通信卫星怎么样给小明发送密码

我们可以举一个简化的例子，假设量子通信卫星给用户小明发送密码。

1. 第一步

此时，它需要先发出一个偏振光子，代表一个比特1或0。

由于光是一种电磁波，光子就是组成光的粒子，电磁波的振动就像绳子抖动一样，可以朝这儿偏也可以朝那儿偏。夏天阳光刺眼，我们戴上墨镜之后，就会觉得对面车窗反射的光线柔和了很多。这是因为偏振墨镜就像一把筛子，把方向与它不一致的偏振光过滤掉了。

量子通信的偏振光子可不是随便偏振的，例如我们规定，朝 0°方向偏振代表比特 0；90°方向偏振代表比特 1。先发出一个偏振光子。

接收光子的“特制墨镜”也不是随便放的，我们规定只能正着放，或者斜着 45°放。假如“特制墨镜”正着放，刚好可以允许 0°方向和 90°方向的光子通过，小明就能顺利接收正确的比特。

2.第二步

假如把“特制墨镜”斜着 45°放呢？按照牛顿力学，0°的光子撞上去肯定是头破血流。但是量子力学可不认这个死理儿，光子哪里有路哪里走。管它正路、斜路，先走两步再说。

这个时候，0°的光子既想从 1 号口子通过，又想从 0 号口子通过，可是小明每次观察它的时候，它只能通过其中一个口子，怎么办呢？上帝也没辙了，只能抛掷骰子决定。掷出来单号就走 1 号口，掷出来双号就走 0 号口，施行单双号通行。90°的光子也一样，得先掷骰子再通行。

100 年以前，量子力学刚刚创立的时候，两个作为创始人的玻尔和爱因斯坦因为这个事还吵了一架。最后，玻尔吵赢了（这一场著名的争吵，后面量子力学那一章再详细讲述）。

于是，我们得到这样一组结论：如果量子通信卫星发射的光子是 0°或 90°的，而小明以 45°斜着摆放“特制墨镜”，他收到的比特就可能是错的。同样的道理，如果量子通信卫星发射的光子是 45°（同样代表比特 0）或 135°（同样代表比特 1）的，而小明正常摆放“特制墨镜”，他收到的比特也可能是错的。只有量子通信卫星发出的光子的偏振方向恰好与小明摆放的“特制墨镜”的方向一样时，小明接收到的比特才是对的。

所以，量子通信卫星每发射一个光子，都要随机选择一组方向：要么是 0°和 90°，要么是 45°和 135°。而小明每次接收光子的时候，也要随机摆放“特制墨镜”：要么正着放，要

么斜着放。这会导致很多比特的传输都是失败的。

上面讲的是100多年前玻尔和爱因斯坦讨论的怎样发送量子比特的事，下面讲现在的事情。

1.7.2　最火的颠覆性技术量子通信在中国

1. 全球首颗量子科学实验卫星“墨子号”成功升空

2016年8月16日，中国研制的量子通信卫星上天了！

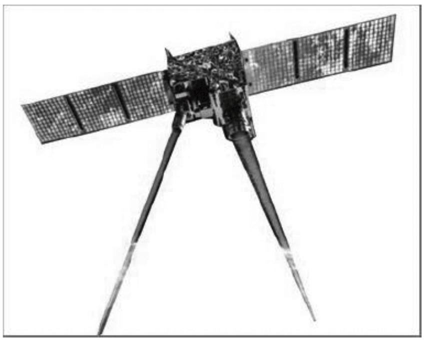


图1-19　全球首颗量子科学实验卫星“墨子号”

从2005年实现13km自由空间量子密钥和纠缠分发，到2016年8月全球首颗量子科学实验卫星“墨子号”（见图1-19）成功升空。再到全球最长的量子保密通信“京沪干线”全线贯通，十余年间，从无到有、从弱到强，我国量子通信技术已跻身全球领先地位，吸引了国际社会的广泛关注。

此前，“墨子号”第一个科学目标已实现并在*Nature*上发表，即在国际上率先实现百万米级星地双向量子纠缠分发和量子力学非定域性检验。

星地高速量子密钥的分发是其第二个目标，通过量子态传输，在遥远两地的用户共享无条件安全的密钥，利用该密钥对信息进行一次一密的严格加密，这是目前人类唯一已知的不可窃听、不可破译的无条件安全的通信方式。

地星量子隐形传态是“墨子号”的第三个科学目标。量子隐形传态是利用量子纠缠将物质的未知量子态精确传送到遥远地点，而不用传送物质本身。

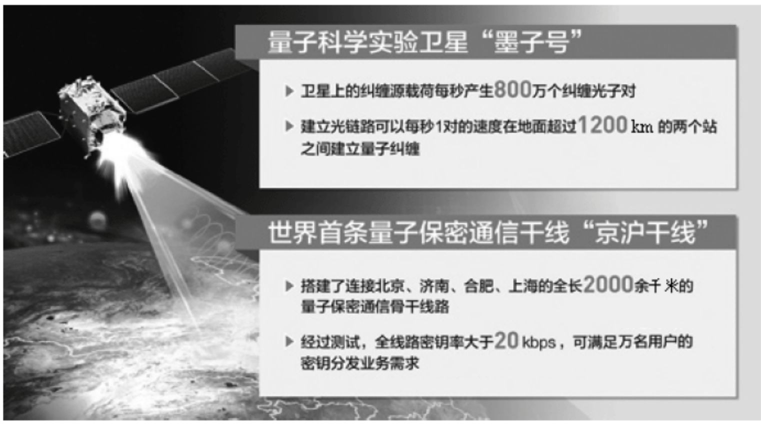
科学家在“墨子号”量子卫星上搭载了自主研发的四种“武器”：量子密钥通信机、量子纠缠发射机、量子纠缠源和量子实验控制与处理机。

同时，在地面建设了科学应用系统，包括一个中心——合肥量子科学实验中心；四个地面站——南山、德令哈、兴隆、丽江量子通信地面站；一个平台——阿里量子隐形传态实验平台。

卫星与地面站共同构成天地一体化量子科学实验系统，在两年的设计寿命期间将进行四大实验任务——星地高速量子密钥分发实验、广域量子通信网络实验、星地量子纠缠分发实验、地星量子隐形传态实验。

实验大致分为三类：第一类是进行卫星和地面之间的量子密钥分发，实现天地之间的安全通信，如果四个地面站任何两两之间都可以实现安全通信，即可实现组网；第二类相当于把量子实验室搬到太空，在空间尺度检验量子理论；第三类是实现卫星和地面百万米量级的量子态隐形传输。

中国量子通信成果如图 1-20 所示。



量子科学实验卫星“墨子号”

- 卫星上的纠缠源载荷每秒产生800万个纠缠光子对
- 建立光链路可以每秒1对的速度在地面超过1200 km 的两个站之间建立量子纠缠

世界首条量子保密通信干线“京沪干线”

- 搭建了连接北京、济南、合肥、上海的全长2000余千米的量子保密通信骨干线路
- 经过测试，全线路密钥率大于20 kbps，可满足万名用户的密钥分发业务需求

图 1-20　中国量子通信成果

以量子密钥分发为核心的量子通信，能够提高用户现有网络传输链路安全等级，是广泛认可的可持续发展的安全通信方案。当前，网络信息安全形势日益复杂，量子通信作为从物理机制上实现无条件安全的信息传输的新型通信方式，对于我国保障网络与信息安全具有重要意义。

2. 量子保密通信“京沪干线”，组网水平全球领先

当前，全球正在加快部署远距离量子通信网络，中国在量子保密通信网络建设方面处于全球领先地位。

量子保密通信“京沪干线”技术验证及应用示范项目开工建设后，干线全长 2000 余千

米，连接北京、上海，贯穿济南、合肥等地，已于2017年8月30日通过总技术验收。与2016年8月16日发射升空的“墨子号”量子科学实验卫星成功对接，标志着全球首个星地一体广域量子保密通信网络雏形初步建立，成功保持了中国量子通信技术实用化的国际领先地位。

“京沪干线”的建成，表明中国在世界上首次实现了基于可信中继方案的远距离量子安全密钥分发，验证了基于异或中继方案的多节点量子密钥安全中继技术、远距离量子保密通信产品的可靠性、大规模量子保密通信网络的管理能力，检验并提升了量子保密通信设备的成熟度与稳定性，推动了量子密钥中继设备、光量子交换机、波分复用等各种信道产品的开发和制造。与国外其他厂商相比，产品更加丰富，在组建多节点的城域网和大型干线网络方面具有明显优势。

自我国量子保密通信“京沪干线”实施以来，主要发达国家和地区在量子通信领域加快战略部署，特别是美国部署了为Google、Microsoft、Amazon公司等互联网巨头数据中心之间的通信提供量子安全保障服务的环美万千米量子保密通信骨干网络；欧盟部署了量子技术旗舰计划支持，并计划在2030年前建成泛欧量子安全互联网；韩国部署了由科学信息通信和未来规划部(MSIP)资助、SK电信牵头计划在2020年建成的韩国国家量子保密通信网络。

1.8 通信编码需要大智慧

1.8.1 解说通信编码

量子通信卫星的一个关键技术是“量子密钥分发”，其实就是一种加密通信，跟发电报、网络支付没什么两样，只不过它生成和发送密码的时候利用了量子力学。

这里说的密码可不是账户的登录密码，而是一种加密信息用的密码。例如，你想加密IBM三个字母，可以规定“把每个字母替换成字母表的相应的前一个字母”，IBM就变成了HAL，“替换成字母表的相应的前一个字母”就是一种加密的密码。

这样的密码太容易破解了，在实战中用的密码则复杂得多。可是密码再复杂又如何，

就跟华山论剑一样,该破的时候还是会破。例如,第二次世界大战的时候,日本海军各个单位都用同一套密码本,其中的密码都是规定死的。一旦敌方缴获了密码本,或者破解了部分密码,就会获取大量军事机密。结果美军破解了密码,摸清了日本海军总司令山本五十六的行踪,导致山本五十六坐飞机时被击落。

德军倒是机灵一点儿。他们设计了一种机器,在运转的时候会产生成千上万种新的密码,叫作恩尼格码密码机,但是对方缴获谜机后,也可以制造专门破解谜机的机器,所以英军破解了谜机,加快了纳粹德国的灭亡。

现代的银行交易和网络支付都使用一种 RSA 加密算法。假如将来有人发明了量子计算机,就完全有可能破解这种算法。

到时候上网购物就麻烦了!所以,传统的密码系统不安全。要想更安全,就得使用物理学家发明的“量子通信密码”。量子通信卫星发送的正是这种密码。

凭什么说量子通信更加安全呢?因为量子通信的密码不是预先规定死的,而是在通信时随机产生的。量子密码分发的三大步如下。

(1)传输一段由0和1组成的随机比特:10100011。

(2)由于量子的随机性,接收方在接收每个比特时,都有一定概率出错:1X10X01X。

(3)双方沟通一下,删除错误的比特,剩下的比特就是随机产生的正确密码。

量子力学可以保证这样的密码不可能被窃听,不可能被破解。

1.8.2 我要说的是“悄悄话”

现代密码学(密码)依赖名为素数因子分解的数学函数。基本上,大数被分解成素数,然后这些素数可以相乘,从而得到大数。经典计算机并不擅长于这方面,要花很长时间才能破解基于素数因子的加密代码。不过你也猜到了,量子计算机确实很擅长于此。

世界各国政府都在竞相制造能够淘汰所有现代形式密码的量子计算机。

为了开发出防止黑客的通信,中国已经将世界上第一颗量子卫星送入轨道,如图1-21所示,这颗卫星的名字叫“墨子”(Micius)。“墨子”旨在研发出远距离量子加密通信。

量子加密是指:使用量子密钥分配(QKD)方法,远距离发送纠缠的光粒子(纠缠光

图 1-21　中国已经将世界上第一颗量子卫星送入轨道

子），以达到确保敏感通信安全的目的。

在 QKD 中，发送方和接收方都通过为每个光子分配 0 或 1，以此测量他们接收到的纠缠光子的极化。使用这种方法创建了量子密钥，而量子密钥可用于加密和解密传输保密信息。

最重要的一点是，如果量子纠缠光子被任何人拦截，系统会立即显示受到干扰的迹象，表明通信不安全。

1. 量子密钥传输偷不走的秘密

以往被认为最安全的信息传递方式是光纤通信。光缆能把所有的光能限制在光纤里，外面得不到能量，所以这个传输被认为是安全的，但随着科技的发展，只需让光缆泄露哪怕很少一部分能量，就能够窃听光缆传递的信号。

科学家表示，这是因为经典通信的信号只有 0 和 1，发生窃听时，这两种信号不会被扰动。比方说，两人打电话时，他人可通过窃听器从通信线路中的上千万个电子中分出一些电子，使其进入另一根线路，从而实现窃听，而通话者无法察觉。美国“棱镜门”等事件的曝光便是最好的例证。

而量子通信则完全不会出现这个情况，这是因为其密钥具有不可复制性和绝对安全性。一旦有人窃取密钥，整个通信信息就会“自毁”并告知使用者。

例如，甲、乙二人要进行安全通信，甲发出的光子信息状态有水平、竖直、45°等，假设有人窃听，由于光子不可分割，首先，窃听者根本无法分割出“半个光子”；其次，因为单次

测量测不准、不可克隆的量子态特性，窃听者无法复制信息；再次，一旦窃听者截获光子，乙就收不到信息，也就不存在窃听。

无论怎样，根据量子力学原理，窃听都可以被发现。一旦被发现，原有密钥立即作废。甲就可以把没有被窃听的密钥传送过去，利用产生的密钥进行完全随机的加密。所以，利用量子不可复制和不可分割的特性可以实现安全量子密钥分发，实现不可破译的保密通信。

换句话说，量子卫星上天后，其发送的每一封信都将是只有天知地知、你知我知的秘密。

2. 量子密码术：帮 Bob（鲍勃）和 Alice（爱丽丝）传悄悄话

Bob 与 Alice，他们是谁？两人什么关系？是不是远隔异地的恋人，每天有说不完的悄悄话？

其实这两个名字，只是在密码学和计算机安全中的惯用角色，他们不一定是“人类”，有可能是一个计算机程序。通常人们都把 Bob 作为发送者，把 Alice 作为接收者，我们后面出现这两个角色时不再解释，以此为准。

20 世纪 80 年代，量子物理学家发现，利用量子力学的基本原理，可以保证信息从 Bob 传给 Alice 的安全性，这就是“量子密码术”。

1）量子密钥分发——最接近实用化的量子技术

量子通信就是利用量子力学基本原理实现信息的传输，而量子保密通信是量子通信的最主要分支，是以保密通信为主要任务，包括量子密钥分发、量子秘密共享和量子安全直接通信三个主要方向。

量子密钥分发模式在 1984 年创立，当时两位科学家班尼特和布拉萨德提出了第一个量子密钥分发协议（BB84 协议），之后 B92、Ekert-91、BBM92 等协议相继提出。目前，已经在实验中实现了 1000 多千米的量子密钥分发，是最接近实用化的量子技术。中国的量子“京沪干线”、量子科学实验卫星等的科学目标之一也是量子密钥分发。

当 Bob 与 Alice 相互发送信息时，量子密钥分发技术通过分发量子密钥能判断是否被窃听，如果没有被窃听，Bob 会将信息发送给 Alice；如果被窃听，Bob 会放弃传输数据。

2）量子秘密共享——Bob 与 Alice 间的第三者

量子秘密共享模式在 1999 年由三位科学家建立，他们提出了这种模式的第一个协议。该技术与量子密钥分发有很大类似性，可以看成是多方参与的量子密钥分发模式。

在量子秘密共享中，Bob 在发送信息给 Alice 时，为了给信息加密，Bob 会在分发密钥给 Alice 的同时，也将密钥分发给第三方，Alice 需要与第三方合作，才能破译 Bob 的密钥，获得传过来的信息内容。

因此，量子秘密共享模式传输的也是随机密钥，需要使用经典通信才能完成信息传送。而量子密钥和量子秘密共享两种技术存在一个问题，人们总是在信息泄露发生之后才能发现窃听存在，而此时窃听者已然获得了信息。为解决这个问题，物理学家们使用一种叫作“一次一密”的方法加密原始信息，但加密后的信息通过普通而非量子的通信信道传送并解密。中国量子科学实验卫星的工作示意图如图 1-22 所示。

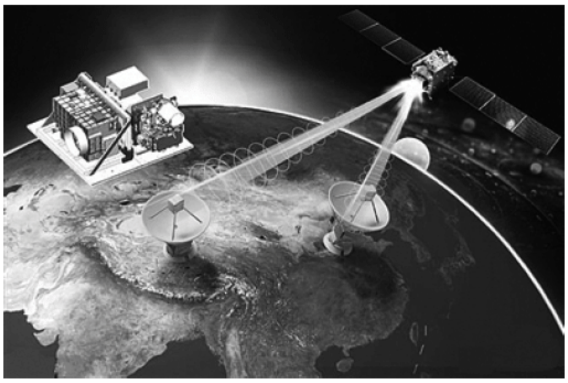


图 1-22　中国量子科学实验卫星的工作示意图

3）量子安全直接通信——在信息泄露前发现窃听

如果物理学家们能够在发送信息之前确保信息传输的安全，能否不使用“一次一密”的方法？量子安全直接通信的模式就不需要事先建立密钥，可利用两个纠缠粒子的量子原理直接传输秘密信息，既能发现窃听，又能保证发现窃听之前的信息不泄露。

该技术的保密原理如下：信息发送者 Alice 留有每对纠缠中的一个光子，把另外一个光子发送给信息接收者 Bob。Bob 把他收到的光子随机分成两组，测量其中的一组光子

并把测量结果公开发给 Alice。Alice 根据测量结果核对传输后的粒子状态有没有被改变,如果改变了,说明被窃听了;如果没有被窃听,那么 Alice 和 Bob 就可以用剩下来的光子直接传输安全信息。

通过理论分析,这样的系统可以实现几十千米的量子安全直接通信。这种方式既可同时作为密钥分发,还可用于构造量子对话、量子签名等新协议,是多用途的量子通信基本协议。

1.9 当今所有密码系统都失效了

1.9.1 量子加密的“不破金身”

量子通信由于量子纠缠态的特性保证了信道内容不会被第三方监听,而密码学问题是为了保证信息保密,信息完整性验证,信息发布的不可抵赖性。量子通信解决了中间人攻击的问题,但是针对传统的泄密、业务逻辑、软件本身存在漏洞这些问题是没有办法解决的。

1. 不可窃听量子通信

前面已经讲了,量子密钥分发的过程中,上帝也没辙了,只好掷骰子决定。抛出单号就走 1 号口,双号就走 0 号口,施行单双号通行。90°的光子也一样,得先掷骰子再通行。就像现在汽车单双号限行。

只要上帝掷骰子,比特传输就有可能出错;只要有出错的可能,这个比特的传输就算失败。随后,把传输失败的比特删掉,只留下传输成功的比特。留下的那一串传输成功的比特,就是在这次量子通信中随机产生的密码。

量子通信中随机产生的密码

10100011

↓

1X10X01X

↓

11001

量子通信传输的密码是不可能被窃听的。因为每次只发送一个光子，假如谁拦截了光子，小明立刻就会发现，就可以马上告诉卫星有人窃听。窃听者也不可能复制出一个一模一样的光子来，因为这会违反“量子不可复制定理”。这种量子通信传输的“套路”，叫BB84协议，也许将来上网剁手会用到。物理学家认为，量子通信可以从根本上解决国防、金融、政务、商业等领域的信息安全问题。

2.量子通信具有很强的保密性

量子具有测量的随机性和不可复制的特性，几乎不可能被破译，以往用微电子技术为基础的计算机技术传递信息极易遭遇窃听。

因为传统通信的密钥都是基于非常复杂的数学算法，只要是通过算法加密的，人们就可以通过计算进行破解。而量子通信则可以做到很安全，不被破译和窃听，这在数学上已经获得了严格的证明。

这种“很安全”是如何实现的？这就要说到在讲量子密钥分发时提到的量子的另外两个特性——测量的随机性和不可复制。

什么是量子测量的随机性？

前面已经讲过，在量子力学里，光子可以朝着某个方向进行振动，叫作偏振。因为量子叠加，一个光子可以同时处在水平偏振和垂直偏振两个量子状态的叠加态。这时，如果你拿一个仪器在这两个方向上进行测量，就会发现每次测量都只会得到其中一个结果：要么是水平的，要么是垂直的。测量的结果完全随机。

在日常的宏观世界里，一个物体的速度和位置，一般是可以同时准确测定的。例如飞机来了，雷达就可以把飞机的速度、位置都准确测定。

在量子世界，测量会破坏或改变量子的状态。如果我们把一个量子的位置测准了，它的速度就测不准了。

既然测量量子的状态会出现随机的结果，那么人们自然也无法对一个不知道其状态的量子进行复制，这就是量子不可复制的特性。

利用这两个特性，量子通信也就保证了安全。在量子密码共享或量子态传递过程中，如果有人窃听，它的状态就会因窃听（测量）发生改变，密码接收的误码率会明显增加，从

而引起发送者和接收者的警觉，而停止该信道的发送。如果窃听者一直在这个信道存在，可以换一个没有发现窃听者的信道重新发送。因为能及时发现窃听者，加上量子的不可复制也使得窃听者无法采取信息复制的方法获得合法用户的信息，所以，量子通信具有很强的保密性。

1.9.2 走近“颠覆性技术”——量子通信能否取代传统通信

量子通信既然这么厉害，那么未来会不会取代传统通信？

答案是：这是两种不同的通信形式，量子通信是为了让传统的数字通信变得更安全。

实际上，量子通信的目标并不是把传统的数字通信取代。例如量子密钥分发，它本身是为了让传统的数字通信变得更安全，并不能独立存在，而量子隐形传态则完全取决于量子计算机的发展。只有未来所有的经典计算机都被量子计算机取代了，才完全会用这种通信方式。但问题是，量子计算机和传统计算机就好比核武器和常规武器，是不可能完全取代彼此的。未来应该是量子通信和传统通信一起构建天地一体化通信网络。

量子通信事关国家信息和国防安全，这个战略性领域已经成为发达国家优先发展的信息科技和产业高地。

美国对量子通信的理论和实验研究开始较早，并最先将其列入国家战略。欧盟则着眼于合力构建量子互联网，2015 年发布《量子宣言》，计划启动 10 亿欧元用于推动量子通信和量子技术的发展。日本也制定了量子信息技术长期发展路线图。

虽然在全球量子通信竞赛中，中国起步并非最早，但是在科学家们的不懈努力下，目前中国在量子通信领域已经实现了“弯道超车”。

中国科技大学团队在 2007 年首次实现安全通信距离超过 100km 的光纤量子密钥分发，2016 年又将安全距离提高到 400km；2016 年中国发射全球首颗量子科学实验卫星；2017 年世界首条量子保密通信干线——“京沪干线”正式开通，希望到 2030 年左右，能建成全球化的广域量子通信网络，并在量子计算领域有所作为。

第 2章

计算机祖孙三代

2.1 计算机爷爷——图灵机模型

2.1.1 艾伦·图灵是个科学家

艾伦·图灵(Alan Turing,1912—1954)如图 2-1 所示。这个名字无论是在计算机领域、数学领域、人工智能领域还是哲学、逻辑学等领域,都可谓掷地有声。艾伦·图灵是计算机逻辑的奠基者,许多人工智能的重要方法也源自这位伟大的科学家。

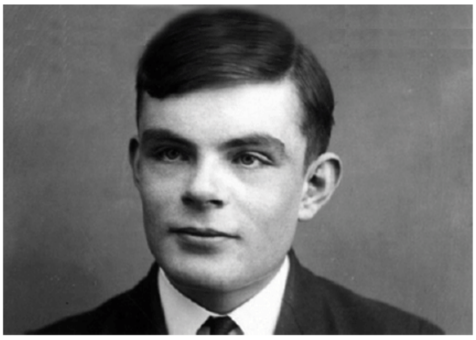


图 2-1 艾伦·图灵

100 多年前,艾伦·图灵诞生在一个文化和科技水平都与现在完全不同的时代里,他为计算机领域奠定了不可埋没的基础,没有他就没有计算机的今天。

他在 24 岁时提出了图灵机理论,31 岁时参与了 Colossus (第二次世界大战时,英国破解德国通信密码的计算机)的研制,33 岁时构思了仿真系统,35 岁时提出自动程序设计

概念，38 岁时设计了“图灵测试”；在后来还创造了一门新学科——非线性力学。他的业余爱好是长跑，如图 2-2 所示。

图 2-2　艾伦·图灵擅长长跑

虽然艾伦·图灵去世时只有 42 岁，但在其短暂而离奇的生涯中的那些科技成就，已让后人享用不尽。人们仰望着这位伟大的英国科学家，把他称为“计算机之父”“人工智能之父”“破译之父”，有人甚至认为，他在技术上的贡献及对未来世界的影响几乎可与牛顿、爱因斯坦等巨人比肩。

1936 年，还在剑桥国王学院就读的艾伦·图灵发表重要论文《论可计算数及其在判定问题上的应用》（*On Computable Numbers, with an Application to the Entscheidungsproblem*），提出“算法（algorithm）”和“计算机（computing machine）”两个核心概念，一直让人们受用到今天。

当时的图灵机还只能计算有限的实数，但它的符号记录方法为以后的计算机发展奠定了基础理论，基于此，人类首次产生了符号处理的概念，并开始把研究重点转向可改变的编码程序，这就是今天软件的前身。

1939 年第二次世界大战爆发，正在为英国国家密码机构工作的艾伦·图灵和其他科学家一起着手研究如何破解敌人的密码，他果然不负众望，成功破译了德国军方使用的著名通信密码系统 Enigma（谜）。于是第一台电子图灵机被设计制造出来，做出重大贡献的艾伦·图灵获得了政府颁发的 OBE 奖。

1946年，艾伦·图灵发表论文阐述存储程序计算机的设计。他的成就与研究离散变量自动电子计算机(Electronic Discrete Variable Automatic Computer)的约翰·冯·诺依曼(John von Neumann)同期。艾伦·图灵的自动计算机与约翰·冯·诺依曼的离散变量自动电子计算机都采用二进制，都以“内存储存程序以运行计算机”打破了那个时代的旧有概念。

1950年，艾伦·图灵的一篇里程碑式的论文《机器能思考吗?》又为人类带来了一个新学科——人工智能。为了证明机器是否能够思考，他又发明了“图灵测试”(Turing Test)，图灵测试在今天仍被沿用。他指出，最好的人工智能研究应该着眼于为机器编制程序，而不是制造机器。而他在论文中预测的计算机发展过程中将会出现的一些问题，至今仍未被解决。

2.1.2　图灵机模型

学习计算机科学的读者都应该知道，在计算机基础理论中有着名的“图灵机”和“图灵测试”。这些理论简洁地概括了图灵伟大贡献的一部分：他是第一个提出利用某种机器实现逻辑代码的执行，以模拟人类的各种计算和逻辑思维过程的科学家。而这一点，成为后人设计实用计算机的思路来源，成为当今各种计算机设备的理论基石。当今计算机科学中再常用不过的程序语言、代码存储和编译等基本概念，就是来自艾伦·图灵的原始构思。

图灵机(Turing Machine)又称为图灵计算机，是艾伦·图灵提出的一种抽象计算模型，即将人们使用纸和笔进行数学运算的过程进行抽象，由一个虚拟的机器替代人们进行数学运算。

图灵机是一个抽象的机器，它有一条无限长的纸带，纸带分成一个一个的小方格，每个方格有不同的颜色；有一个机器头在纸带上移来移去。机器头有一组内部状态，还有一些固定的程序。在每个时刻，机器头都要从当前纸带上读入一个方格信息，然后结合自己的内部状态查找程序表，根据程序输出信息到纸带方格上，并转换自己的内部状态，然后进行移动。

2.1.3 计算机界的诺贝尔奖

图灵奖(Turing Award)是美国计算机协会(ACM)于1966年设立的,专门奖励那些对计算机事业做出重要贡献的个人。其名称取自世界计算机科学的先驱、英国科学家、英国曼彻斯特大学艾伦·图灵,这个奖设立目的之一是纪念这位现代计算机奠基者。获奖者必须是在计算机领域具有持久且重大的先进性的技术贡献。大多数获奖者是计算机科学家。

图灵奖是计算机界最负盛名的奖项,有“计算机界的诺贝尔奖”之称。图灵奖对获奖者的要求极高,评奖程序也极严,一般每年只奖励一名计算机科学家,只有极少数年度有两名以上在同一方向上做出贡献的科学家同时获奖。

2.2 所有计算机的同一祖宗——图灵机

艾伦·图灵是第一个提出制造一种简单的计算机想法的人。图灵机的操作仅局限于读写磁带上的符号,将磁带移向左边或右边来一次读取一个符号。这个发明常被认为是计算机时代的开端。

实际上,“可计算的”一词的定义是一个可以由图灵机来解决的问题。图灵机还在翻译和破解用恩尼格码密码机写码的德国信息方面起着很大作用。

前面提到过,艾伦·图灵写了一篇名为《论可计算书机器判定问题上的应用》的论文,这就是艾伦·图灵享誉世界很重要的论文之一。可能当时连他也不会想到,这篇文章中所提到的概念最终使他从数学和逻辑学系统中开辟出一个全新的分支——计算机。

1. 图灵机的概念

接下来介绍一下图灵机的概念(值得注意的是,图灵机只是一个概念,并不是一个实体机器)。

图灵机的基本思想如图2-3所示,图灵机由一条无限长的纸带(tape)、读写头(head)、一套控制读写头移动规则的规则表(table)和一个状态寄存器(register)组成。

艾伦·图灵的基本思想是用机器模拟人们用纸和笔进行数学运算的过程，他把这样的过程看作下列两种简单的动作。

（1）在纸上写上或擦除某个符号。

（2）把注意力从纸的一个位置移到另一个位置。

而在每个阶段，人要决定下一步的动作，依赖于：①此人当前所关注的纸上某个位置的符号；②此人当前思维的状态。

2.图灵机的运算过程

为了模拟人的这种运算过程，艾伦·图灵构造出一台假想的机器，该机器由以下几个部分组成。

（1）一条无限长的纸带，如图 2-4 所示。

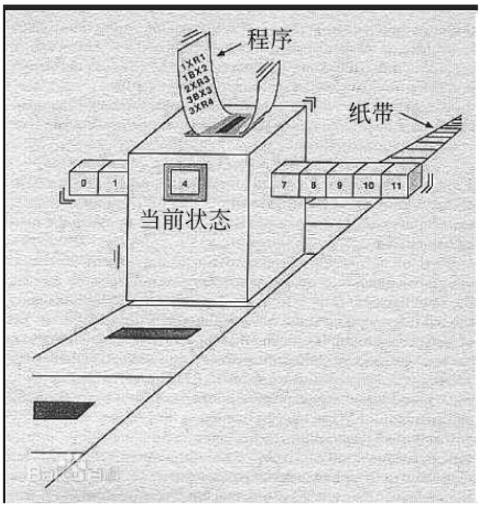

程序
1XR1
1BX2
2XR3
3BX3
3XR4
纸带
0
1
4
当前状态
7
8
9
10
11

图 2-3　图灵机的基本思想

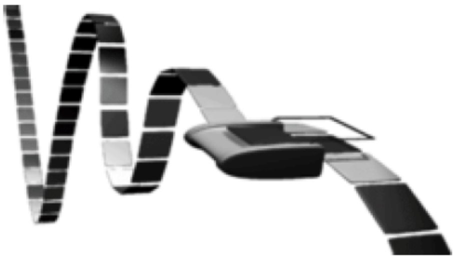


图 2-4　图灵机的艺术表示

纸带被划分为一个接一个的小格子，每个格子上包含一个来自有限字母表的符号，字母表中有一个特殊的符号表示空白。纸带上的格子从左到右依此被编号为 0、1、2 等，纸带的右端可以无限伸展。

（2）一个读写头。

读写头可以在纸带上左右移动，它能读出当前所指的格子上的符号，并能改变当前格子上的符号。

（3）一套控制规则表。

控制规则根据当前机器所处的状态以及当前读写头所指的格子上的符号确定读写头下一步的动作，并改变状态寄存器中的值，令机器进入一个新的状态。

（4）一个状态寄存器。

状态寄存器用来保存图灵机当前所处的状态。图灵机的所有可能状态的数目是有限的，并且有一个特殊的状态，称为停机状态。

注意：这个机器的每一部分都是有限的，但它有一个潜在的无限长的纸带，因此，这种机器只是一个理想的设备。艾伦·图灵认为这样的一台机器就能模拟人类所能进行的任何计算过程。

图 2-5 中所示纸带被分为无限个格子，可记录任何字母、二进制数字（0，1）及空白。每个格子里代表了图灵机的输入和输出信息，空白则表示没有任何信息。下方三角为读写头，表示当前读写（输入输出）的位置。读写头可向左右移动，每次移动一个格。

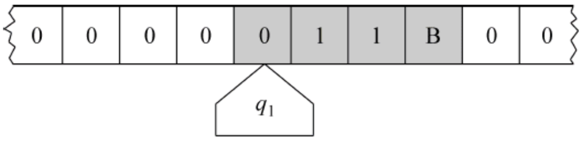


图 2-5　图灵机的结构

在某些模型中，读写头沿着固定的纸带移动。要进行的指令（q_1）展示在读写头内。在这种模型中“空白”的纸带全部为 0。有阴影的方格，包括读写头扫描到的空白，标记了“1，1，B”的那些方格，以及读写头符号，构成了系统状态。

其移动方向由当下读写头所指的输入和规则表决定（规则表其实就是当时控制计算机的程序）。读写头首先记录下当下位置的状态（q_1）并存入状态寄存器，然后根据当下输入对比程序中的要求进行左右移动或停留在当下位置，最后根据程序输出字母或数字，修改新位置的数字或字母。每次工作图灵机的读写头都会从起始位置开始，由规则表和输

入控制其移动到不同位置，并最终在程序结束时停留在空白格里。

3. 图灵机的意义

细心的读者会发现，图灵机的整个构想已经满足现代计算机所需要的所有基本元素，包括程序、输入输出和存储器，如图 2-6 所示。

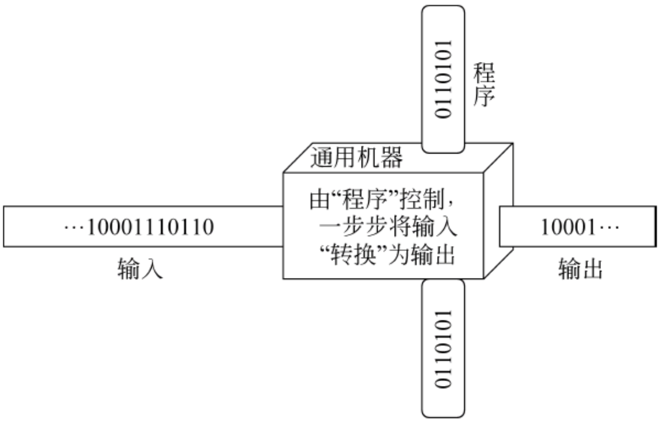

0110101
程序
通用机器
由“程序”控制，
一步步将输入
“转换”为输出
…10001110110
输入
10001…
输出
0110101

图 2-6　图灵机的构想满足了现代计算机所有基本元素

这也是为什么说图灵机奠定了现代计算机发展的基础。因为现在计算机能做的一切事情图灵机都可以做到（图灵机的具体工作示例会在后面慢慢提到）。

2.3　计算机爸爸——冯·诺依曼机

2.3.1　第一个“攒”计算机的人——冯·诺依曼

冯·诺依曼（见图 2-7），原籍匈牙利，布达佩斯大学数学博士。20 世纪最重要的数学家之一，在现代计算机、博弈论、核武器和生化武器等领域内都有建树，被后人称为“计算机之父”和“博弈论之父”。

他先后执教于柏林大学和汉堡大学，1930 年前往美国，后入美国籍。历任普林斯顿大学、普林斯顿高级研究所教授，美国原子能委员会会员，美国全国科学院院士。早期以算子理论、共振论、量子理论、集合论等方面的研究闻名，开创了冯·诺依曼代数。

第二次世界大战期间为第一颗原子弹的研制做出了贡献。为研制电子数字计算机提供了基础性的方案。1944 年与莫根斯特恩合著《博弈论与经济行为》,这是博弈论学科的奠基性著作。晚年,研究自动机理论,著有对人脑和计算机系统进行精确分析的著作——《计算机与人脑》。

主要著作有《量子力学的数学基础》《计算机与人脑》《经典力学的算子方法》《博弈论与经济行为》《连续几何》等。

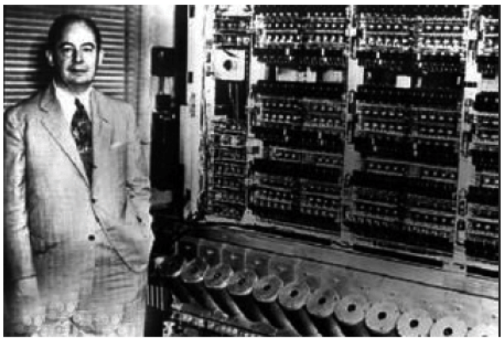


图 2-7　冯·诺依曼

冯·诺依曼对世界上第一台电子计算机 ENIAC(Electronic Discrete Variable Automatic Computer,电子数字积分计算机)的设计提出过建议,1945 年 3 月他在共同讨论的基础上起草了一个全新的“存储程序通用电子计算机方案”——EDVAC。这对后来计算机的设计有决定性的影响,特别是确定计算机的结构,采用存储程序以及二进制编码等,至今仍为电子计算机设计者所遵循。如图 2-8 所示,冯·诺依曼(右)和其合作者在世界上第一台计算机前。

众所周知,1946 年发明的电子计算机,大大促进了科学技术以及社会生活的进步。鉴于冯·诺依曼在发明电子计算机中所起到的关键性作用,被西方人誉为“计算机之父”。而在经济学方面,他也有突破性成就,被誉为“博弈论之父”。

在物理领域,冯·诺依曼在 20 世纪 30 年代撰写的《量子力学的数学基础》已经被证明对原子物理学的发展有极其重要的价值。他在化学方面也有相当的造诣,曾获苏黎世高等技术学院化学系的大学学位。他无愧是 20 世纪最伟大的全才之一。

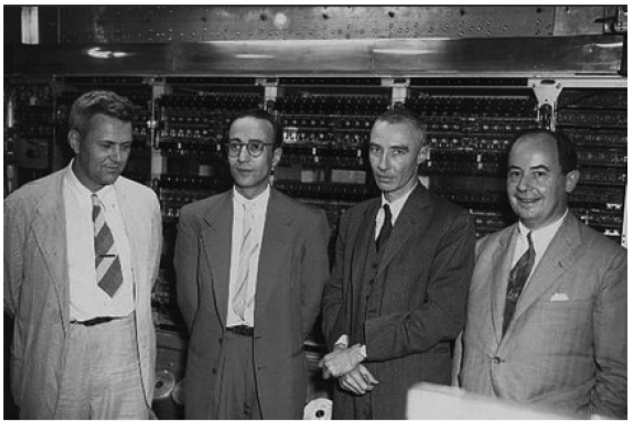


图 2-8 冯·诺依曼(右)等在世界上第一台计算机前

2.3.2 经典计算机的五脏六腑

一般认为,ENIAC是世界第一台电子计算机,它由美国科学家研制,于1946年2月14日在费城开始运行。其实由汤米·费劳尔斯等英国科学家研制的科洛萨斯(Colossus)计算机比ENIAC机问世早两年多,于1944年1月10日在布莱奇利园区开始运行。ENIAC机证明,电子真空技术可以大大地提高计算技术。

1944年,冯·诺依曼参加原子弹的研制工作,该工作涉及极为困难的计算。在对原子核反应过程的研究中,要对一个反应的传播做出“是”或“否”的回答。解决这一问题通常需要几十亿次的数学运算和逻辑指令,尽管最终的数据并不要求十分精确,但所有的中间运算过程均不可缺少,且要尽可能保持准确。他所在的实验室为此聘用了一百多名女计算员,利用台式计算机从早到晚计算,还是远远不能满足需要。无穷无尽的数字和逻辑指令如同沙漠一样把人的智慧和精力吸尽,冯·诺依曼想到了使用ENIAC解决这一问题。

不过,ENIAC本身存在两大缺点:一是没有存储器;二是它用布线接板进行控制,甚至要搭接几天,计算速度也就被这一工作抵消了。冯·诺依曼发现了ENIAC的最大弱点——没有真正的存储器。ENIAC只有20个暂存器,它的程序是外插型的,指令存储在计算机的其他电路中。这样,解题之前必须先想好所需的全部指令,通过手工把相应的电

路连好。这种准备工作要花几小时甚至几天，而计算本身只需几分钟。计算的高速与程序的手工之间存在很大矛盾。

针对这个问题，冯·诺依曼提出程序内存的思想：把运算程序存在机器的存储器中，程序设计员只需要在存储器中寻找运算指令，机器就会自行计算，这样，就不必每个问题都重新编程，从而大大加快了运算进程。这一思想标志着自动运算的实现，标志着电子计算机的成熟，已成为电子计算机设计的基本原则。

冯·诺依曼以“关于EDVAC的报告草案”为题，起草了长达101页的总结报告。报告广泛而具体地介绍了制造电子计算机和程序设计的新思想。这份报告是计算机发展史上一个划时代的文献，它向世界宣告：电子计算机的时代开始了。如图2-9所示，冯·诺依曼和奥本海默在第一台计算机前合影。

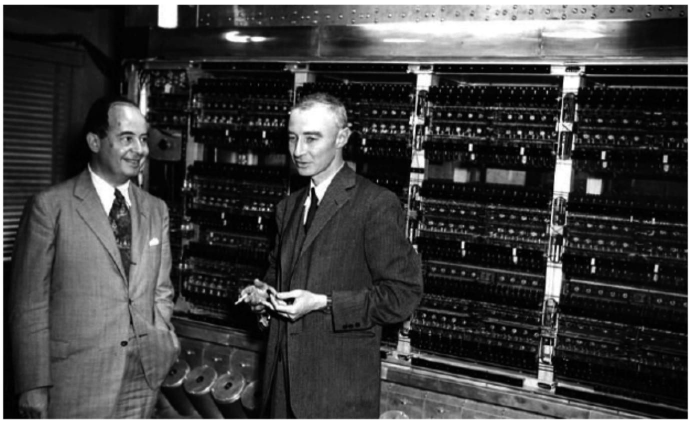


图2-9　冯·诺依曼和奥本海默在第一台计算机前合影

EDVAC方案明确奠定了新机器由5个部分组成，包括运算器、控制器、存储器、输入和输出设备，并描述了这五部分的职能和相互关系。报告中，冯·诺依曼对EDVAC中的两大设计思想做了进一步的论证，为计算机的设计树立了一座里程碑。

设计思想之一是二进制，他根据电子元件双稳态工作的特点，建议在电子计算机中采用二进制。报告提到了二进制的优点，并预言，二进制的采用将大大简化机器的逻辑线路。

计算机基本的工作原理是存储程序和程序控制。

实践证明了冯·诺依曼预言的正确性。如今，逻辑代数的应用已成为设计电子计算机的重要手段，在EDVAC中采用的主要逻辑线路也一直沿用着，只是对实现逻辑线路的工程方法和逻辑电路的分析方法做了改进。

2.3.3　经典计算机的工作“门道”

1. 冯·诺依曼体系结构

从20世纪初，物理学和电子学科学家们就在争论制造可以进行数值计算的机器应该采用什么样的结构。人们被十进制这个人类习惯的记数方法所困扰。所以，那时以研制模拟计算机的呼声更为响亮和有力。20世纪30年代中期，冯·诺依曼大胆提出，抛弃十进制，采用二进制作为数字计算机的数制基础。同时，他还说预先编制计算程序，然后由计算机按照人们事前制定的计算顺序执行数值计算工作。

冯·诺依曼理论的要点是：数字计算机的数制采用二进制；计算机应该按照程序顺序执行。

人们把冯·诺依曼的这个理论称为冯·诺依曼体系结构。从ENIAC（ENIAC并不是冯·诺依曼体系结构）后到当前最先进的计算机都采用的是冯·诺依曼体系结构，如图2-10所示。所以，冯·诺依曼是当之无愧的“数字计算机之父”。

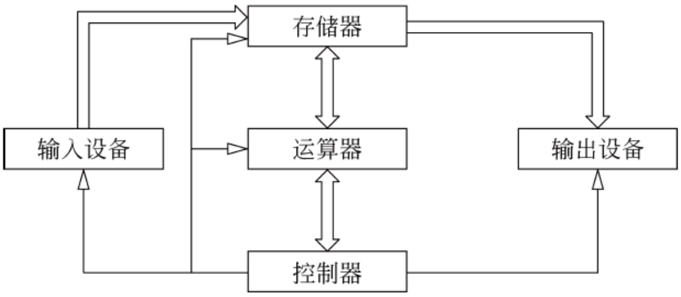


图2-10　电子计算机的基本结构图

图2-10中，单线箭头为控制指令流向，双向箭头为数据流向。

根据冯·诺依曼体系结构构成的计算机，必须具有如下功能。

（1）把需要的程序和数据送至计算机中。

（2）必须具有长期记忆程序、数据、中间结果及最终运算结果的能力。

（3）能够完成各种算术、逻辑运算和数据传送等数据加工处理的能力。

（4）能够根据需要控制程序走向，并能根据指令控制机器的各部件协调操作。

（5）能够按照要求将处理结果输出给用户。

为了完成上述功能，计算机必须具备五大基本组成部件。

（1）输入数据和程序的输入设备。

（2）记忆程序和数据的存储器。

（3）完成数据加工处理的运算器。

（4）控制程序执行的控制器。

（5）输出处理结果的输出设备。

冯·诺依曼的主要贡献就是提出并实现了“存储程序”的概念。由于指令和数据都是二进制码，指令和操作数的地址又密切相关，因此，当初选择这种结构是很自然的。但是，这种指令和数据共享同一总线的结构，使得信息流的传输成为限制计算机性能的瓶颈，影响了数据处理速度的提高。

在典型情况下，完成一条指令需要 3 个步骤，即取指令、译码和执行，如图 2-11 所示。

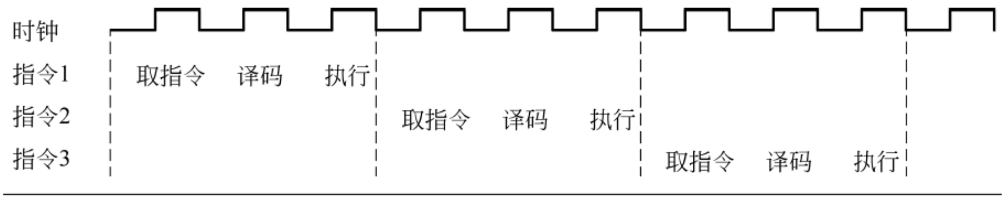


图 2-11　指令流的定时关系

从指令流的定时关系也可看出冯·诺依曼结构的特点。举一个最简单的例子，对存储器进行读写操作的指令，指令 1 至指令 3 均为存、取数指令，对冯·诺依曼结构处理器，由于取指令和存取数据要从同一个存储空间存取，经由同一总线传输，因而它们无法重叠执行，只有一个完成后再进行下一个。

2.计算机中央处理器体系结构

实际上，中央处理器的体系架构并不是只有冯·诺依曼结构一家，目前主流的架构可

以分为冯·诺依曼结构和哈佛结构。

1）冯·诺依曼结构

使用冯·诺依曼结构的中央处理器和微控制器有很多。除了Intel公司的中央处理器，ARM的ARM7处理器、MIPS公司的MIPS处理器也采用冯·诺依曼结构。

人们把利用这种概念和原理设计的电子计算机系统统称为“冯·诺依曼型结构”计算机。冯·诺依曼结构的处理器使用同一个存储器，经由同一个总线传输。

冯·诺依曼结构的处理器具有以下几个特点：必须有一个存储器；必须有一个控制器；必须有一个运算器，用于完成算术运算和逻辑运算；必须有输入和输出设备，用于进行人机通信。

2）哈佛结构

哈佛结构是一种将程序指令存储和数据存储分开的存储器结构。中央处理器首先到程序指令存储器中读取程序指令内容，解码后得到数据地址，再到相应的数据存储器中读取数据，并进行下一步的操作（通常是执行）。程序指令存储和数据存储分开，可以使指令和数据有不同的数据宽度，如Microchip公司的PIC16芯片的程序指令是14位宽度，而数据是8位宽度。

哈佛结构的微处理器通常具有较高的执行效率。其程序指令和数据指令分开组织和存储，执行时可以预先读取下一条指令。使用哈佛结构的中央处理器和微控制器有很多，除了上面提到的Microchip公司的PIC系列芯片，还有Zilog公司的Z8系列、Atmel公司的AVR系列和ARM公司的ARM9、ARM10和ARM11。

哈佛结构是指程序空间和数据空间独立的体系结构，目的是为了减轻程序运行时的访存瓶颈。

例如，最常见的卷积运算中，一条指令同时取两个操作数，在流水线处理时，同时还有一个取指操作，如果程序和数据通过一条总线访问，取指和取数必会产生冲突，而这对大运算量的循环的执行效率是很不利的。哈佛结构能基本上解决取指和取数的冲突问题。而对另一个操作数的访问，就只能采用增强哈佛结构了，例如像TI那样，数据区再分割，并多一组总线。

哈佛结构处理器有两个明显的特点：使用两个独立的存储器模块，分别存储指令和数据，每个存储模块都不允许指令和数据并存；使用独立的两条总线，分别作为 CPU 与每个存储器之间的专用通信路径，而这两条总线之间毫无关联。

3）冯·诺依曼结构与哈佛结构的区别

根据冯·诺依曼体系结构组成的计算机，其所具有的功能前面已讲过，这里不再赘述。

哈佛结构是为了高速数据处理而采用的。因为可以同时读取指令和数据（分开存储的），大大提高了数据吞吐率，缺点是结构复杂。通用微机指令和数据是混合存储的，结构上简单，成本低。假设是哈佛结构：你就得在计算机上安装两块硬盘，一块装程序，一块装数据；内存装两根，一根储存指令，一根存储数据……

至于优缺点，哈佛结构复杂，对外围设备的连接与处理要求高，十分不适合外围存储器的扩展。所以早期通用 CPU 难以采用这种结构，而单片机，由于内部集成了所需的存储器，所以采用哈佛结构也未尝不可。

2.4 计算机孙子——量子计算机

量子计算机（quantum computer）是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息，运行的是量子算法时，它就是量子计算机。

2.4.1 量子计算机的起源

早期的量子计算机，实际上是用量子力学语言描述的经典计算机，并没有用到量子力学的本质特性，如量子态的叠加性和相干性。

在经典计算机中，基本信息单位为比特，运算对象是各种比特序列。与此类似，在量子计算机中，基本信息单位是量子比特，运算对象是量子比特序列。所不同的是，量子比特序列不但可以处于各种正交态的叠加态上，而且还可以处于纠缠态上。这些特殊的量

子态，不仅提供了量子并行计算的可能，而且还将带来许多奇妙的性质。

与经典计算机不同，量子计算机可以做任意的幺正变换，在得到输出态后，进行测量得出计算结果。因此，量子计算对经典计算进行了扩充，在数学形式上，经典计算可看作是一类特殊的量子计算。

1982 年，美国著名物理物学家理查德·费曼在一个公开的演讲中提出利用量子体系实现通用计算的新奇想法。紧接其后，1985 年，英国物理学家大卫·杜斯提出量子图灵机模型。理查德·费曼当时就想到，如果用量子系统所构成的计算机模拟量子现象则运算时间可大幅度减少，从而量子计算机的概念诞生了。

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。其基本规律包括不确定原理、对应原理和玻尔理论等。

量子计算机的优越性表现在：量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，并按一定的概率振幅叠加起来，给出量子计算机的输出结果。这种计算称为量子并行计算，也是量子计算机最重要的优越性。

2.4.2　量子计算机的研究历史

量子计算/量子计算机的概念是费曼于 1982 年首先提出的。费曼还在微型机械(Tiny Machine)的课堂上首先提出纳米科学这一个概念，他课堂上的学生某种意义是人类第一批纳米科学家。然后又一个新领域诞生了。所以，现在美国的纳米科学领域的奖叫作费曼纳米技术奖。

理查德·费曼提出量子计算/量子计算机的概念，一开始是从物理现象的模拟而来的。他发现当模拟量子现象时，因为庞大的希尔伯特空间(多维抽象空间)使资料量也变得庞大，一个完好的模拟所需的运算时间变得相当可观，甚至是不切实际的天文数字。理查德·费曼当时就想到，如果用量子系统构成的计算机模拟量子现象，则运算时间可大幅度减少。量子计算机的概念从此诞生。

但是量子计算机，或推而广之的量子资讯科学，在 20 世纪 80 年代多处于理论推导等纸上谈兵状态。

1994年，贝尔实验室的专家Shor提出量子质因子分解算法后，因其对通行于银行及网络等处的RSA加密算法破解而构成威胁后，量子计算机变成了热门的话题。除了理论之外，也有不少学者着力于利用各种量子系统实现量子计算机。

1995年，Shor提出大数因子分解的量子算法，这时，大家才认识到量子计算机的超强计算能力，特别是破解编码的能力，之后就有很多学者加入这方面的研究。

2007年2月，加拿大D-Wave公司宣布研制成功16个量子比特的超导量子计算机，但其作用仅限于解决一些最优化问题，与科学界公认的能运行各种量子算法的量子计算机仍有较大区别。

2009年11月15日，世界首台可编程的通用量子计算机正式在美国诞生。同年，英国布里斯托尔大学的科学家研制出基于量子光学的量子计算机芯片，可运行Shor算法。

2011年4月，一个成员来自澳大利亚和日本的科研团队在量子通信方面取得突破，实现了量子信息的完整传输。同年9月，科学家证明量子计算机可以用冯·诺依曼架构实现。

2017年5月，IBM公司发布17量子比特的处理器，并宣布正研发50量子比特原型机，量子计算商业化加速。

2017年10月，Intel公司交付49量子比特测试芯片，其计算能力等于5000颗8代Intel i7。

2017年，Google公司宣布开源量子计算软件OpenFermion。

2017年，加拿大量子计算公司D-Wave发布全球第一款商用型量子计算机D-Wave 2000Q。

人们研究量子计算机最初很重要的一个出发点是探索通用计算机的计算极限。这些行走在人类能力圈边缘的天才物理学家们总是有着这梦幻般的创作力。所思所想皆对人类做出巨大贡献。量子计算的发展历史如图2-12所示。

2.4.3 量子计算机算法理论

1. 量子计算机的经典算法

半导体靠控制集成电路记录及运算信息，量子计算机则希望控制原子或小分子的状

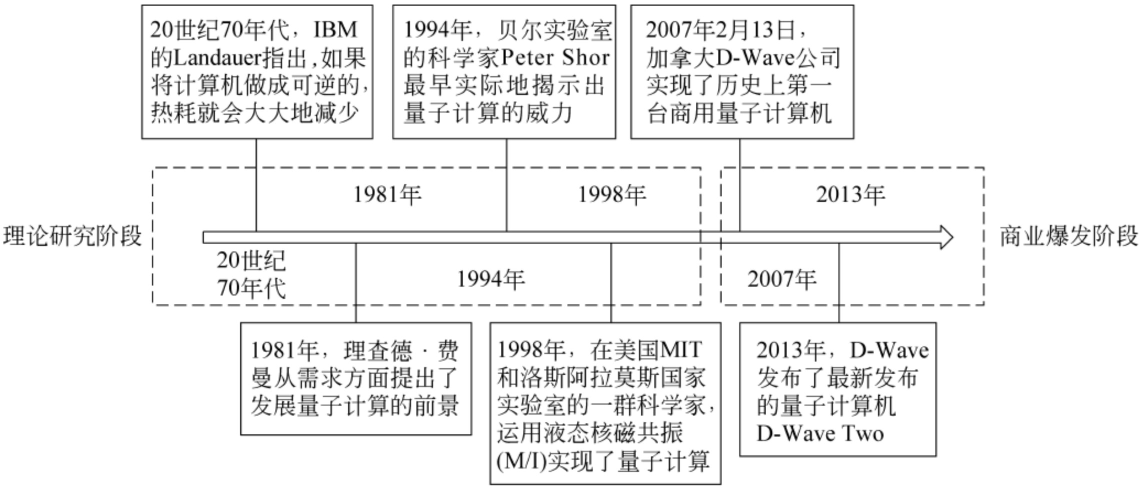

20世纪70年代，IBM的Landauer指出，如果将计算机做成可逆的，热耗就会大大地减少
1994年，贝尔实验室的科学家Peter Shor最早实际地揭示出量子计算的威力
2007年2月13日，加拿大D-Wave公司实现了历史上第一台商用量子计算机
1981年
1998年
2013年
理论研究阶段
商业爆发阶段
20世纪70年代
1994年
2007年
1981年，理查德·费曼从需求方面提出了发展量子计算的前景
1998年，在美国MIT和洛斯阿拉莫斯国家实验室的一群科学家，运用液态核磁共振(M/I)实现了量子计算
2013年，D-Wave发布了最新发布的量子计算机D-Wave Two

图 2-12　量子计算机的发展历史

态，记录和运算信息。1994 年，贝尔实验室的专家 Peter Shor 证明量子计算机能做出离散对数运算，而且速度远胜传统计算机。因为量子不像半导体只能记录 0 和 1，可以同时表示多种状态。如果把半导体比成单一乐器，量子计算机就像交响乐团，一次运算可以处理多种不同状况，因此，一个 40 比特的量子计算机，就能在很短时间内解开 1024 位计算机花数十年解决的问题。

2. 量子计算机通用计算

顾名思义，量子计算机就是实现量子计算的机器，是一种使用量子逻辑进行通用计算的设备。不同于电子计算机，量子计算用来存储数据的对象是量子比特，它使用量子算法进行数据操作。

要说清楚量子计算，首先看经典计算机。经典计算机从物理上可以被描述为对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路来实现。

(1) 其输入态和输出态都是经典信号，用量子力学的语言描述，即其输入态和输出态都是某一力学量的本征态，如输入二进制序列 0110110。

(2) 经典计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质，因此，经典计算机中的变换(或计算)只对应一类特殊集。

相应于经典计算机的以上两个限制，量子计算机分别进行了推广。量子计算机的输入用一个具有有限能级的量子系统描述，如二能级系统（称为量子比特），量子计算机的变换（即量子计算）包括所有可能的幺正变换。

（1）量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交。

（2）量子计算机中的变换为所有可能的幺正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。

承载16量子比特的硅芯片如图2-13所示。

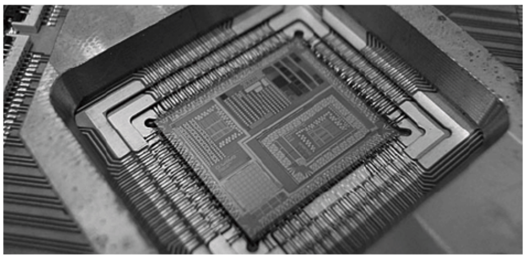


图2-13　承载16量子比特的硅芯片

由此可见，量子计算对经典计算进行了极大扩充，经典计算是一类特殊的量子计算。量子计算最本质的特征为量子叠加性和量子相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成量子并行计算。

无论是量子并行计算还是量子模拟计算，本质上都是利用了量子相干性。遗憾的是，在实际系统中量子相干性很难保持。在量子计算机中，量子比特不是一个孤立的系统，它会与外部环境发生相互作用，导致量子相干性的衰减，即消相干（也称为“退相干”）。因此，要使量子计算成为现实，一个核心问题就是克服消相干。

量子编码是迄今发现的克服消相干最有效的方法。主要的几种量子编码方案是量子纠错码、量子避错码和量子防错码。量子纠错码是经典纠错码的类比，是目前研究的最多的一类编码，其优点为适用范围广，缺点是效率不高。

3. 保密通信与密码破解

正如大多数人所了解的，量子计算机在密码破解上有巨大潜力。

当今主流的非对称(公钥)加密算法(如RSA加密算法)大多数都是基于于大整数的因式分解或者有限域上的离散指数的计算这两个数学难题。它们的破解难度也就依赖于解决这些问题的效率。

传统计算机上,要求解这两个数学难题,花费时间为指数时间(即破解时间随着公钥长度的增长以指数级增长),这在实际应用中是无法接受的。

为量子计算机量身定做的Shor算法可以在多项式时间内(即破解时间随着公钥长度的增长以k次方的速度增长,其中k为与公钥长度无关的常数)进行整数因式分解或者离散对数计算,从而为RSA、离散对数加密算法的破解提供可能。

其他不是基于这两个数学问题的公钥加密算法,例如椭圆曲线加密算法,量子计算机还无法进行有效破解。

针对对称(私钥)加密,如AES加密算法,只能进行暴力破解,传统计算机的破解时间为指数时间,而量子计算机可以利用Grover算法进行更优化的暴力破解,量子计算机暴力破解AES-256加密的效率跟传统计算机暴力破解AES-128是一样的。

更广泛而言,Grover算法是一种量子数据库搜索算法,相比传统的算法,达到同样的效果,它的请求次数要少得多。对称加密算法的暴力破解仅仅是Grover算法的其中一个应用。

量子计算机除了解密之外,还有保密通信的作用,在利用EPR对(二粒子纠缠态:两个粒子间距离多远,一个粒子的变化都会影响另一个粒子的现象,即两个粒子之间不论相距多远,从根本上讲它们还是相互联系的)进行量子通信的实验中我们发现,只有拥有EPR对的双方,才可能完成量子信息的传递,任何第三方的窃听者都不能获得完全的量子信息。正所谓解铃还须系铃人,这样实现的量子通信,才是真正不会被破解的保密通信。

此外,量子计算机还可以用来做量子系统的模拟,人们一旦有了量子模拟计算机,就无须求解薛定谔方程或者采用蒙特卡罗方法在经典计算机上做数值计算,便可精确地研究量子体系的特征。

25　量子计算机的“硬件单元”已经造出来了

量子计算的原理实际上应该分为两部分：一部分是量子计算机的物理原理和物理实现；另一部分是量子算法。

下面大致地说一下量子计算机的物理原理和物理实现现状。

首先，现在不存在类似于经典计算机的量子通用计算机。现有的有实际意义的硬件就两种：量子退火机和量子模拟机。

量子退火机的技术细节比较复杂，而且除了D-Wave公司的人和少数的合作者，其他人对这一块都不熟悉。因为是商业公司，所以D-Wave公司跟学界的交流不太多，基本上处于半技术垄断状态。

D-Wave公司非常擅长解决二次非约束二进制优化问题（Quadratic Unconstrained Binary Optimization，QUBO）。一旦找到这种映射，那么人们就不再需要关心如何设计方法得到最优解，因为量子绝热过程会自动地到达基态，也就是最优解，理论上可以保证全局最优。

量子退火机是目前唯一拥有商业价值的量子计算机。它只能解决QUBO问题，但是有相当多的经典问题可以归约成QUBO问题，所以还是有实际意义的。而且现在有几千比特，已经能满足很多现实问题的需求了。目前计算的瓶颈主要在于如何用经典计算机快速转化成QUBO。

人们平常说的量子计算机主要是指量子模拟机。所谓模拟，就是用经典方法控制一个量子系统，从而模拟量子过程，即量子-量子模拟。虽然模拟机可以完成所有量子计算过程，但这与量子通用计算机是不一样的。

量子模拟机主要有两个问题：一是模拟机需要庞大的经典控制系统，而且缺乏量子-经典的反馈过程；二是结构过于简单，算不上计算机，短时间内看不到通用量子计算的希望，但是模拟机造大一点，做一些量子模拟对化学、生物的帮助还是很大的，可以模拟一些经典计算机无法模拟的大分子，如蛋白质。Google公司的量子霸权主要针对的就是这个

问题，49 量子比特可以模拟的量子系统就跟世界排名靠前的超级计算机能模拟的一样大，所以 Google 公司把 50 量子比特叫作量子霸权（超过现存的所有经典计算机）。

量子模拟机的硬件部分非常随意，现有的实现方法很多，总有人能想出些奇怪的实现方案。主流的有光量子、核磁共振、光学腔、离子阱、超导等。

2.5.1 量子计算机的硬件单元

1. 量子寄存器

存储一系列量子比特的体系称为量子寄存器。假设有一个由 3 比特构成的寄存器，在经典计算机中，可以表示 0～7 共 8 个数，并且在某一时刻，只能表示其中的一个数。

000	001	010	011
100	101	110	111

对量子寄存器来说，若此寄存器是由量子比特构成，每个量子比特可以处于$|0\rangle$或$|1\rangle$或$|0\rangle$与$|1\rangle$的叠加态，即在某时刻一个量子存储器可以同时表示 8 个数。

$|0\rangle|0\rangle|0\rangle+|0\rangle|0\rangle|1\rangle+|0\rangle|1\rangle|0\rangle+|0\rangle|1\rangle|1\rangle+|1\rangle|0\rangle|0\rangle+|1\rangle|0\rangle|1\rangle+|1\rangle|1\rangle|0\rangle+|1\rangle|1\rangle|1\rangle$

3 量子比特的系统如图 2-14 所示。

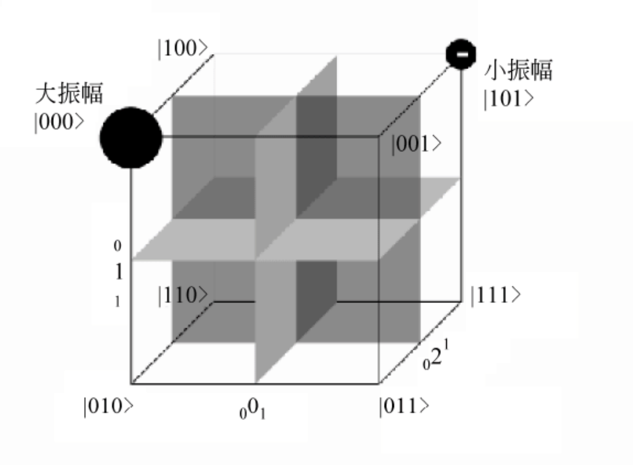


图 2-14 3 量子比特的系统

3 量子比特的系统可以同时表示 8 个传统状态，如图 2-15 所示。

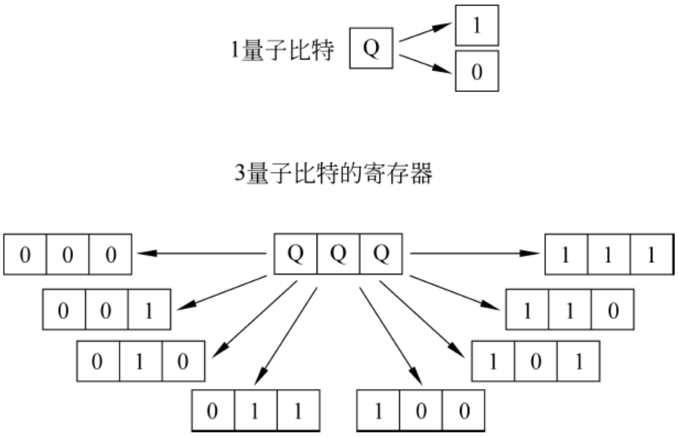


图 2-15　3 量子比特的系统可以同时表示 8 个传统状态

2. 量子逻辑门

量子逻辑门是一个对特定的量子比特在一段时间间隔实现逻辑变换的量子逻辑线路，它是量子线路的基础。与传统逻辑门不同，量子逻辑门是可逆的。

量子逻辑门是量子计算与量子计算机实现的基础，可用下列方法实现。

（1）量子点系统。

（2）超导约瑟夫森结系统。

（3）核磁共振量子系统。

（4）离子阱系统。

（5）腔量子电动力学系统等。

在经典计算机中，逻辑判断是按真值表进行，任何逻辑运算均可以归类于 3 项基本的布尔操作：非（NOT）、与（AND）、或（OR）。这些基本的逻辑运算称为门。

与经典计算机的门相对应。量子计算机中的量子门由幺正变换实施。

量子逻辑门按照其作用的量子比特的数目可分为单比特门、二比特门和三比特门等。其中，常用的单比特门有哈达玛门 Hadamard（简记为 H）、Pauli-X 门、Pauli-Y 门等；常用的二比特门有可控非门（Controlled-NOT）、对换门（Swap）等；常用的三比特门有三位非

门（Toffoli）等。

量子门的真值表比经典的真值表要广泛得多，量子门是实现量子并行计算的基石。

可以作为实现量子计算的通用逻辑门的 Fredkin 门的真值表如图 2-16 所示。

输入比特			输出比特		
A (target)	B (target)	C (control)	A (target)	B (target)	C (control)
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	1	1
1	0	1	0	0	1
1	1	1	1	1	1
1	0	1	0	0	1
1	1	1	1	1	1

图 2-16　Fredkin 门的真值表

Toffoli 门如图 2-17 所示。

Toffoli 门的真值表如图 2-18 所示。

异或（XOR）门及其对应操作如图 2-19 和图 2-20 所示。

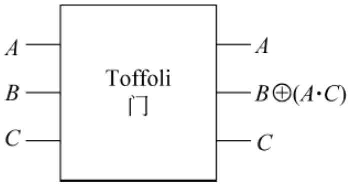


图 2-17　Toffoli 门

输入比特			输出比特		
A (control)	B (control)	C (target)	A (control)	B (control)	C (target)
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

图 2-18　Toffoli 门的真值表

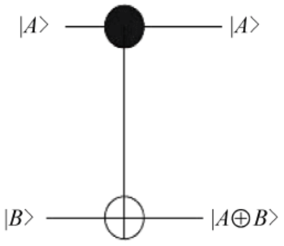


图 2-19　异或（XOR）门

$$
\begin{aligned}
U_{\mathrm{XOR}}|0,0\rangle &= |0,0\rangle \\
U_{\mathrm{XOR}}|0,1\rangle &= |0,1\rangle \\
U_{\mathrm{XOR}}|1,0\rangle &= |1,1\rangle \\
U_{\mathrm{XOR}}|1,1\rangle &= |1,0\rangle
\end{aligned}
$$

图 2-20　异或（XOR）门对应操作

将量子门按某种方式连接，构成量子网路，以进行复杂的运算。例如，利用 XOR 门与转动门构成的 Toffolli 门如图 2-21 所示。

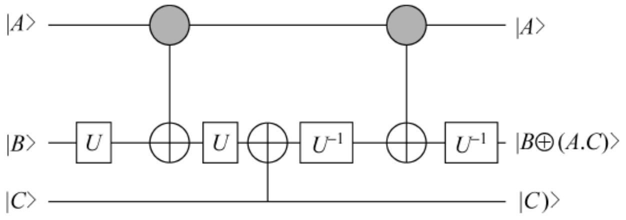

|A>
|A>
|B>
U
U
U⁻¹
U⁻¹
|B⊕(A.C)>
|C>
|C)>

图 2-21　利用 XOR 门与转动门构成的 Toffolli 门

3. 量子网路

例如，K 位寄存器上做分离（快速）傅里叶变换的公式及量子网路如图 2-22 和图 2-23 所示。

$$|a\rangle \rightarrow \frac{1}{\sqrt{k}} \sum_{c=0}^{k-1} e^{j2\pi c/K} |c\rangle$$

图 2-22　分离（快速）傅里叶变换

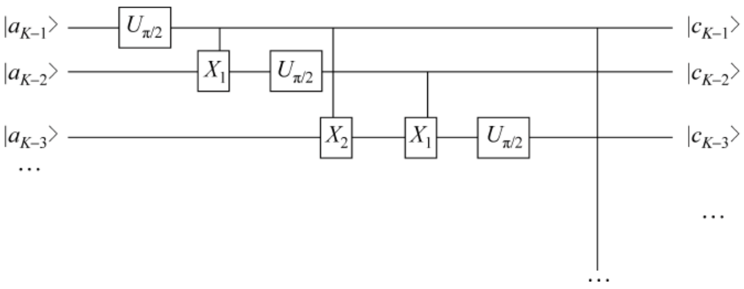

|a_{K-1}>
|a_{K-2}>
|a_{K-3}>
…
U_{π/2}
X_1
U_{π/2}
X_2
X_1
U_{π/2}
|c_{K-1}>
|c_{K-2}>
|c_{K-3}>
…
…

图 2-23　K 位寄存器上做分离（快速）傅里叶变换的量子网路

2.5.2　量子计算机的硬件逻辑单元是用什么材料做成的

其实所谓的逻辑单元，也就是量子比特，就是一个能进行相干操作的二能级系统。按照这个标准，很多物理体系都可以做量子比特。不同的量子比特有不同的优点和限制，这里不详述。

简单地说，量子计算机首先需要物理载体实现量子比特，再根据具体载体的特点实现通用的门操作。一般实验室中，常见的物理载体大概有以下 5 种。

1. 线性光学系统

一般利用光子的偏振/路径编码比特，利用波片/偏振片等实现门操作。优点是光子因为没有相互作用，噪声影响小，但也因此缺少集成性。自量子信息这一领域兴起时，一直是演示各种方案的平台，但不太可能做出实用的通用计算机。

2. 核磁共振

利用核自旋编码比特，通过精确的脉冲电磁信号实现门操作。这个系统比较干净，操作精度高，所以早期发展很快。但它本质上只能实现系综操作（无法操作某个单一比特，而是一次操作非常多数量的比特），并且同样缺乏扩展性，目前也淡出量子计算机发展方向，大部分时候是作为演示平台使用。

3. 金刚石色心

利用色心的电子自旋编码。这个系统发展的时间不长，优势在于室温下可控，但也缺乏集成性。在精密/灵敏测量方向的应用比较活跃，如磁场测量。

4. 离子阱

利用离子某些稳定的能级编码比特，以离子之间的运动模式实现耦合，激光实现囚禁和操控。目前发展比较活跃，当前思路是把它做到芯片上以实现更大规模的集成。但由此面临噪声变强和寻址困难的问题。

5. 超导比特

这是人工构建的系统，利用非简并（非简并指的是物理体系处于一个能级所对应的可

能状态和相应波函数是唯一的)的能级作为比特,微波实现门操作。因为技术脱胎于现代光刻技术,所以天然在集成性上有优势。早期因为系统本身噪声很大,所以没有受到很大的重视。这些年,由于开发出新的比特架构,对抗噪声的时间有了数量级的提升,是Google、IBM公司大力投资的系统。Google公司宣称在2017年年末利用这一系统,解决了经典计算机无法解决的问题。

其他诸如超晶格系统在计算方面的研究不是很活跃;至于拓扑量子计算,目前载体尚不清楚,虽然理论上这种计算有天然的容错性。

总之,目前离通用量子计算机的突破还是有比较大距离的,所以未必有确定的路线图。比较可能的是,在未来几年,某些具体的优化/模拟问题上,上述一些物理系统可能会提供超过经典计算机的能力。

2.5.3 新型量子计算机首个基本元件问世

据报道,瑞典和奥地利物理学家携手,研制出了单量子比特里德伯(Rydberg)门,这是新型量子计算机——囚禁里德伯离子量子计算机的首个基本元件。单量子比特里德伯门扩展性更强、运算速度更快,最新研究证明了建造这种量子计算机的可行性,其有潜力克服目前的量子计算方法面临的扩展问题。

目前,量子计算机面临的最大问题之一是,如何增加每个逻辑门中发生纠缠的量子比特的数量,这对于开发出实用的量子计算设备至关重要。升级之所以困难,部分原因在于囚禁离子的系统内常用的多量子比特逻辑门,会随着量子比特数量的增加而遭遇“频谱拥挤”问题。然而,囚禁里德伯离子的系统不受频谱拥挤问题的影响,这表明,以囚禁里德伯离子作为量子比特而研制的量子计算机,或许能成为升级能力更强的量子计算机。

研究人员在最新发表的论文中称,他们建造出了首个单量子比特里德伯门。他们估计,可将这一单量子比特系统扩展到二量子比特系统,未来还可以添加更多量子比特。

除了潜在的升级优势,基于囚禁里德伯离子而研制的量子计算机还拥有其他优势,包括能更好地控制量子比特、门运算速度更快等。

2.5.4　世界上第一个完整的量子计算机芯片设计揭晓

澳大利亚新南威尔士大学（UNSW）科学家小组已经在量子计算的大规模应用方面取得了重大突破。通过改造微处理器的架构，科学家们创造了一个完整的量子计算机芯片的第一个设计，允许使用硅基材料进行量子计算。互补金属氧化物半导体（CMOS）的这些标准工业部件是所有现代电子设备设计中的关键部分。

新的量子计算机芯片设计可以为处理数百万个“量子比特”铺平道路，它使用与标准微处理器中用于选择位的操作相似的操作。简单地说，芯片的设计基本上可以描述当今台式机、笔记本计算机或iPhone等开放式智能手机平台执行量子操作时使用的相同工程路径。

不同的是，涉及工程的量子操作部分是量子比特。与传统计算机中的标准“比特”不同，作为超级版本的比特，量子比特提供了指数级的更多处理能力。

虽然在量子力学中也认为“叠加”的两态性质使量子计算机比传统计算机快，但缺点是在叠加态下实现和维持量子比特是非常困难的。事实上，物理学家目前一般仅能够处理在芯片上少于50个稳定的量子比特。

虽然这是量子计算领域的一个重大成就，但实际上，成千上万，甚至数百万量子比特是实现大规模量子技术所必需的。目前有限的量子比特封装芯片能力有限的原因在于量子比特存在于一个微妙的、类似禅宗的叠加状态中，这使得它们非常脆弱，不稳定并容易出错。隔壁摇摆原子的任何微小推动都可能使它们失去平衡。除非量子比特连接到定义其性质的系统，否则即使是最轻微的环境干扰也会被放大到错误的答案。

为了克服这个问题并使量子比特更强健，澳大利亚科学家小组提出了新的纠错码，允许多个量子比特存储单个数据。芯片蓝图整合了一种专门为自旋量子比特设计的新型纠错码，并且涉及在数百万量子比特上操作的复杂协议。这是第一次尝试将所有常规硅电路集成到一个芯片中，以控制和读取量子计算所需的数百万个量子比特。

随着科学家朝着芯片的最初制造流程迈进，将会进一步进行设计修改。量子计算所需的所有关键组件都在一块芯片上。

这是创造大规模量子计算机的一个巨大的技术飞跃。当量子计算达到我们今天看到的与智能手机相当的实际水平时，世界变化的技术不仅能在几分钟内完成目前计算机需要几千年的任务，而且还将引导人类发现和设计新的拯救生命的药物治疗，以难以置信的精确性帮助解决最棘手的科学问题，创造出不可动摇、超级强大的个人计算机，探索宇宙的奥秘。

2.6　量子计算机里面还得有“软件算法”

2.6.1　量子计算机的算法理论

传统计算机靠控制集成电路记录和运算信息，量子计算机则希望控制原子或小分子的状态，记录和运算信息。

量子计算机是实现量子计算的机器，是一种使用量子逻辑进行通用计算的设备。不同于传统电子计算机，量子计算用来存储数据的对象是量子比特，它使用量子算法进行数据操作。

要说清楚量子计算，首先看经典计算机和量子计算机的区别。

1. 经典计算机的特征

经典计算机从物理上可以被描述为对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路实现。

（1）其输入态和输出态都是经典信号，用量子力学的语言来描述，即其输入态和输出态都是某一力学量的本征态。例如，输入二进制序列 0110110，用量子记号，即 $|0110110\rangle$。所有的输入态均相互正交。对经典计算机不可能输入如下叠加态：$C1|0110110\rangle + C2|1001001\rangle$。

（2）经典计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质，因此，经典计算机中的变换（或计算）只对应于一类特殊集。

2. 量子计算机的特征

相应于经典计算机的以上两个限制，量子计算机分别做了推广。量子计算机的输入

用一个具有有限能级的量子系统来描述，如二能级系统（称为量子比特），量子计算机的变换（即量子计算）包括所有可能的幺正变换。

（1）量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交。

（2）量子计算机中的变换为所有可能的幺正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。

3. 经典计算是一类特殊的量子计算

由此可见，量子计算对经典计算做了极大的扩充，经典计算只是一类特殊的量子计算。量子计算最本质的特征为量子叠加性和量子相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，量子并行计算。

2.6.2　为量子计算机量身定做的Shor算法

正如大多数人所了解的，量子计算机在密码破解上有巨大潜力。当今主流的非对称（公钥）加密算法，如RSA加密算法，大多数都是基于大整数的因式分解或者有限域上的离散指数的计算这两个数学难题。它们的破解难度也就依赖于解决这些问题的效率。传统计算机上，要求解这两个数学难题，花费时间为指数时间（即破解时间随着公钥长度的增长以指数级增长），这在实际应用中是无法接受的。

例如，1234乘以3433容易算出来，但计算4 236 322的因子就不那么容易了。分解一个数的质因子的计算复杂度随该数增长而迅速膨胀。破解RSA129（有129位阿拉伯数字）时，花费了1600位因特网用户8个月的时间。密码破译者认为，更多的数字应当被加到密钥中以抵抗计算机性能的增长（这将花费比宇宙年龄还长的时间计算RSA140）。然而，对于使用运行Shor算法的一台量子计算机，密钥中的阿拉伯数字个数对问题的难度有着极小的影响。破译RSA140只需花费几秒钟。

为量子计算机量身定做的Shor算法是由美国贝尔实验室科学家Shor（见图2-24）在1994年提出的分解大数质因子的量子方法。可以在有限时间内进行整数因式分解或者离散对数计算，从而

图2-24　Peter Shor

为 RSA、离散对数加密算法的破解提供可能。

假设以对 N 进行分解为例，设数 N 在二进制中位数为 L。

Shor 算法是一种随机运算法，但因量子计算具有高度并行能力，每次运算可同时处理 2^{2L} 个数据。

设经典计算机的运算速度约 10^{12} 次/秒，进行 10^{30} 次运算需 10^{18} s，而宇宙的寿命约为 10^{17} s，即意味着到我们所处的宇宙终结，计算仍旧没有结果。在量子计算机上采用量子算法，同样的运算速度，10^{-8} s 可完成。

Shor 发明的算法能够快速地分解大数字。它将会对密码系统有着深刻的影响，它会威胁到由公钥密码学所提供的安全性（例如 RSA）。

但其他不是基于这两个数学问题的公钥加密算法，如椭圆曲线加密算法，量子计算机还无法进行有效破解。

2.6.3 量子并行计算的随机搜索——Grover 算法

量子计算机里面还有另外一种著名的量子并行计算的随机搜索——Grover 软件算法，我们先从算法的数学原理看 Grover 算法是如何并行计算的。

1997 年，Grover 发现了另一种很有用的量子搜寻算法，这也是一种量子计算的经典算法，它适用于解决如下问题：从 N 个未分类的客体中寻找出某个特定的客体。

经典算法只能是一个接一个地搜寻，直到找到所要的客体为止，这种算法平均地讲要寻找 $N/2$ 次，成功概率为 1/2。

例如，要从有 100 万个号码的电话本中找出某个指定号码，该电话本是以姓名为顺序编排的。经典方法是一个个找，平均要找 50 万次，才能以 1/2 概率找到所要电话号码。Grover 算法是每查询一次可以同时检查所有 100 万个号码。

由于 100 万量子比特处于叠加态，量子干涉的效应会使前次的结果影响下一次的量子操作，这种干涉生成的操作运算重复 1000（即 $\sqrt{\mathrm{N}}$）次后，获得正确答案的概率为 1/2。但若再多重复操作几次，那么找到所需电话号码的概率接近于 1。

Grover 算法的用途很广，可以寻找最大值、最小值、平均值等，也可以用于下棋。最

有趣的是可有效地攻击密码体系，如 DES 体系，这个问题的实质是从 $n=2^{56}\approx 7\times 10^{16}$ 个可能的密钥中寻找一个正确的密钥。若以每秒 100 万密钥的运算速率操作，经典计算需要 1000 年，而采用 Grover 算法的量子计算机则只需小于 4min。

更广泛而言，Grover 算法是一种量子数据库搜索算法，相比传统的算法，达到同样的效果，它的请求次数要少得多。对称加密算法的暴力破解仅仅是 Grover 算法的其中一个应用。

2.7 量子计算机展望

1. 量子计算机展望

量子计算机是实现量子计算的机器，它是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。量子计算机以处于量子状态的原子作为中央处理器和内存，应用的是量子比特，可以同时处于多个状态。

迄今为止，世界上还没有真正意义上的量子计算机。但是，世界各地的许多实验室正在以巨大的热情追寻这个梦想。

如何实现量子计算，方案并不少，问题是在实验上实现对微观量子态的操纵确实太困难了。已经提出的方案主要利用了原子和光腔相互作用、冷阱束缚离子、电子或核自旋共振、量子点操纵、超导量子干涉等。还很难说哪一种方案更有前景，只是量子点方案和超导约瑟夫森结方案更适合集成化和小型化。

现在的实验只制备出单个量子逻辑门，远未达到实现计算所需要的逻辑门网络。科学家也只能同时控制约 10 量子比特，量子计算机至少需要几十量子比特才能解决现实世界中的问题，进而成为一种可行的计算方式。

将来也许现有的方案都派不上用场，最后脱颖而出的是一种全新的设计，而这种新设计又是以某种新材料为基础。

实现量子计算的另一个困难是可集成性问题，可集成性最核心的问题不是将几个量子比特组装到一起，而是能相干地操控这些量子比特。

作为量子计算机最终实现的要求，量子比特体系要有长的相干时间，基本的门操作的

精度要能够达到容错量子计算的阈值之内。这是最核心的技术指标，只有这个目标实现了，才能实现真正意义上的多位量子计算机，从而物理体系的可集成性最终才能体现价值。

研究量子计算机的目的不是用它来取代现有的计算机。量子计算机使计算的概念焕然一新，这是量子计算机与其他计算机（如光计算机和生物计算机等）的不同之处。量子计算机的作用不只是解决一些经典计算机无法解决的问题。

2.量子计算机就要来了，它真能改变世界吗

量子计算机的理论运行速度远远超出任何传统的超级计算机。量子计算机或将使得人们在原子层面对物质状态进行模拟成为可能，从而可以重塑新材料技术；量子计算机也可以通过无穷的算力破解现有的任何加密算法，重新定义网络安全；量子计算机甚至能够通过对海量数据的有效处理来增强人工智能的水平。

经过几十年的逐步发展，研究人员终于离打造出真正的量子计算机无限接近了，其强大的功能足以打败任何传统意义上的计算机，这就是具有里程碑意义的“量子霸权”（quantum supremacy）。目前来看，Google 公司在该领域一直处于领导地位，而诸如 Intel 和 Microsoft 等公司也都在努力跟进，包括 Rigetti Computing、IonQ 和 Quantum Circuits 等有雄厚资金支持的创业公司也在迎头赶上。

大家都在尝试寻找这些问题的答案：量子计算机到底有什么好处？我们是否可以打造一款实用的、可靠的量子计算机？

量子物理学的发展已经有一个世纪的历史，但整个计算科学仍然依赖于经典物理学和克劳德・艾尔伍德・香农（Claude Elwood Shannon ）于 20 世纪 50 年代在麻省理工学院开发的信息数学理论。香农根据存储数据所需的比特数量（这是一个普及但没有确定的术语）来定义信息量。这些比特，也就是二进制码的 0 和 1 是所有常规计算科学的基础。

20 世纪 70 年代，相关领域的科学家奠定了量子信息理论的基础，这会挑战传统计算科学。它以原子尺度上物体的特殊性质为基础。在这个微观尺度下，粒子可以一次显现出许多种状态（例如，许多不同的位置），也就是“叠加”态。两个粒子也可能表现出“量子

纠缠”，因此，改变一个粒子的状态可能会瞬间影响另一个粒子的状态。

在量子现象的帮助下，可以有效地执行几种耗时甚至不可能的计算。量子计算机会将信息存储在量子比特中。量子比特可以以 1 和 0 叠加的形式存在，并且可以使用量子纠缠和量子干涉找到指数级大数据计算的解决方案。但是目前还难以比较量子计算机相比于经典计算机到底有多大的计算优势，粗略地说，只有几百个量子比特的量子计算机能够同时执行的计算量要比已知宇宙中的原子数量多。

1981 年夏天，IBM 公司和麻省理工学院组织了一次名为“计算物理第一次会议”的里程碑式活动。计算科学和量子物理史上最有影响力的几位大人物悉数出席了此次会议。其中包括开发第一台可编程计算机的康拉德・楚泽以及量子理论的主要贡献者理查德・菲利普斯・费曼。费曼在会上发表了主题演讲，其中提到了使用量子效应进行计算的想法。他说：“自然是量子的，该死的！所以如果我们想模拟它，需要一台量子计算机。”

2016 年，IBM 公司将一台小型量子计算机连接到云端（见图 2-25）。用户使用称为 QISKit 的编程工具包可以在云上运行简单的程序。成千上万的人已经开发了运行基本量子算法的 QISKit 程序。现在 Google 和其他公司也在将它们的量子计算机联网。现在不能用量子计算机做很多事情，但至少可以尝试一下可能会发生的事情。

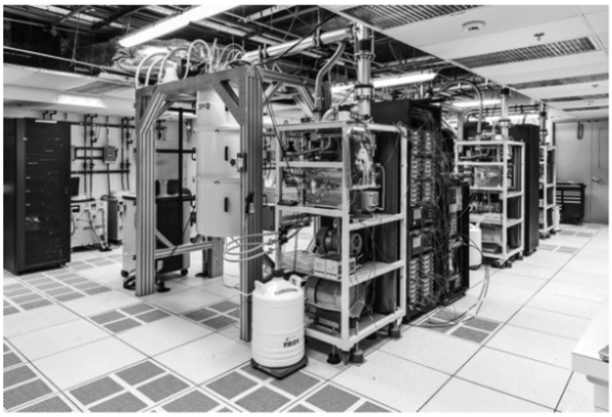


图 2-25　IBM 公司将量子计算机连接至云端

IBM 公司的量子计算机是现存最有前途的计算机。该机器被用于创建和操纵量子计算机中的基本元素：存储信息的量子比特。

3. 梦想与现实之间的差距

IBM 公司的量子计算机利用了超导材料中发生的量子现象。例如,有时超导材料中的电子会同时进行顺时针和逆时针的移动,这就是量子现象。IBM 公司的量子计算机使用了超导电路,其中两个不同的电磁能量状态组成量子比特。

超导方法具有关键优势。其中的硬件可以使用现有的完善制造方法制造出来,并且能够通过传统的计算机控制整个系统。超导电路中的量子比特比单个光子或离子更容易操作,也没有那么敏感。

在量子实验室里,工程师们正在研究一个具有 50 量子比特的计算机。人们可以在一台普通的计算机上运行简单的量子计算机模拟系统,但是不可能模拟多达 50 量子比特。这意味着理论上量子计算机可以解决传统计算机无法解决的问题奇点:换句话说,也就是量子霸权。

但正如研究人员所说,量子霸权是一个难以捉摸的概念。量子计算机需要 50 量子比特全部正常运行才能够起作用,而实际上量子计算机却被需要纠正的错误所困扰。在任何时间长度内维持量子比特的状态都非常困难;它们倾向于“退货”,或者失去其微妙的量子特性,就像烟圈会在最轻微的气流中散开一样。量子比特越多就越发困难。

耶鲁大学教授、Quantum Circuits 公司的创始人罗伯特·舍尔科普夫(Robert Schoelkopf)表示,“如果你有 50 或 100 量子比特可以正常运行,又能够实现完全纠错,那么你就可以进行前所未有的计算,任何传统计算机都无法复制的计算。”“量子计算的另一个问题在于,它出错的方式是指数级的。”

另一个值得注意的问题是,即使是堪称完美的量子计算机作用也并不明显。它并不会简单地加快任务处理速度;事实上,对于许多计算来说,量子计算机的执行速度比传统机器还要慢。迄今为止,只有少数特别设计的算法在量子计算机中具有显著优势。即使对于这些算法来讲,优势也往往是短暂的。

最著名的量子算法是由 Shor 在麻省理工学院开发的关于计算质因数分解问题的算法。许多常见的密码方案都依赖于传统计算机难以实现的现实,但是密码学可以进行自适应调整,创造出不依赖于因数分解的新型加密代码。

即便已经接近50量子比特的历史临界点，但IBM公司的研究人员依旧热衷于消除关于量子计算机的炒作问题。量子计算机设备比在传统计算机上进行的模拟要复杂得多，但它的精度还无法控制，因为你并不十分清楚该如何应对量子算法。赋予研究人员希望的是这样一种情况，那就是不完善的量子计算机也可能是有用的。

研究人员已经注意到费曼在1981年设想的应用，例如，化学反应和材料性质取决于原子和分子之间的相互作用。这些相互作用受量子现象的支配。量子计算机至少在理论上可以模拟出常规方法无法处理的那些模型。以前，研究人员已经使用7量子比特的机器模拟氢化铍的精确结构。虽然仅仅只有三个原子，但它是用量子系统建模的最复杂分子。最终，研究人员可能会使用量子计算机来设计更高效的太阳能电池、更有效的药物或将阳光转化为清洁燃料的催化剂。

这些目标的实现还有很长的路要走。但是，人们或将能够从一台与经典计算机配对的易错量子计算机中获得有价值的结果。人们正处于一个巨大起点之上——量子计算最终将在人工智能中发挥作用。量子计算机不但需要不同的编程语言，而且需要根本不同的思维方式编程。

国际创业社区对量子计算机也越来越兴奋。量子创业公司的一场竞赛已经开始，一群初创公司企业家正向一群教授和投资者展示他们的想法：一家公司希望用量子计算机来模拟金融市场；另一家公司则计划用量子计算机来设计新的蛋白质；还有一家公司想要开发更高级的人工智能系统。一切皆有可能，但唯一可以得到确认的是，每个团队的业务都建立在一种革命性的技术基础上，而这种技术几乎不存在。人们的猜测是，第一批实用量子计算机的诞生还有几年的时间。同时，这也要假设管理和操纵大量量子比特并不是一个棘手问题。但是，几乎没有人会因为这个事实而感到害怕。

第3章

牛顿力学的困境及飞跃

3.1 物理大家族

由伽利略(1564—1642)和牛顿(1642—1727)等于17世纪创立的经典物理学,经过18世纪在各个基础部门的拓展,到19世纪得到了全面、系统和迅速的发展,达到了它辉煌的顶峰。到19世纪末,已建成了一个包括力、热、声、光、电等学科在内的、宏伟完整的理论体系。特别是它的三大支柱——经典力学、经典电动力学、经典热力学和统计力学——已臻于成熟和完善,不但在理论的表述和结构上已十分严谨和完美,而且它们所蕴含的十分明晰和深刻的物理学基本观念,对人类的科学认识也产生了深远的影响。

3.1.1 经典物理学的建立发展过程

人们在高中上的物理课都是基于伽利略和牛顿等科学家创立的经典物理学理论。

按物理学自身发展的特点分期,可以把物理学的发展分为若干时期,在每一时期中找出一些具有表征性的特点。这主要是根据物理学发展的内在逻辑分期的,采用这一分期原则既可兼顾社会生产和社会经济形态的影响,又能揭示贯穿于物理学发展过程中的内在规律性。

按照物理学本身发展的规律,结合社会经济各时期的特点,并考虑不同时期有不同的研究方法,把物理学发展的历史大体分为三个时期。

1. 经验物理

经验物理时期(17世纪以前)内,我国和古希腊形成两个东西交相辉映的文化中心。

经验科学已从生产劳动中逐渐分化出来，这时期的主要方法是直觉观察与哲学的猜测性思辨。与生产活动及人们自身直接感觉有关的天文、力、热、声、光（几何光学）等知识首先得到较多发展。除希腊的静力学外，中国在以上几方面在当时都处于领先地位。在这个时期，物理学尚处在萌芽阶段。

2. 经典物理

经典物理学时期（17 世纪初—19 世纪末）资本主义生产促进了科学与技术的发展，形成了比较完整的经典物理学体系。系统的观察实验和严密的数学推导相结合的方法，被引进物理学中，导致了 17 世纪主要在天文学和力学领域中的“科学革命”。牛顿力学体系的建立，标志着经典物理学的诞生。经过 18 世纪的准备，物理学在 19 世纪获得了迅速和重要的发展。终于在 19 世纪末以经典力学、热力学和统计物理学、经典电磁场理论为支柱，使经典物理学的发展达到了顶峰。

3. 现代物理

现代物理学时期指 20 世纪初至今。19 世纪末叶物理学上一系列重大发现，使经典物理学理论体系本身遇到了不可克服的危机，从而引起现代物理学革命。由于生产技术的发展，精密、大型仪器的创制以及物理学思想的变革，这一时期的物理学理论呈现出高速发展的状况。研究对象由低速到高速，由宏观到微观，深入到广垠的宇宙深处和物质结构的内部，对宏观世界的结构、运动规律和微观物质的运动规律的认识，产生了重大变革。

3.1.2　物理学的危机

19 世纪是经典物理学的峥嵘岁月，是一个构建科学理论大厦的时代，是理论与实验完美结合的时代，产生了很多著名的物理学家。科学技术发展突飞猛进，并产生了广泛的社会影响，由力学、电磁学、热学、光学、声学构建经典物理学的大厦。也可以说 19 世纪是经典物理学的辉煌时代。

物理学发展到 19 世纪末期，可以说已经达到了相当完美、成熟的程度。物理学的辉煌成就，使得不少物理学家踌躇满志、沉溺于欢快陶醉之中，于是产生了这样一种看法：物理学的大厦已经落成，今后物理学家用不着再干什么了，只需要把各种数据测得精确些

就行了。

1900年新春之际，著名物理学家开尔文勋爵在送别旧世纪的讲演中讲道：“19世纪已将物理学大厦全部建成，今后物理学家的任务就是修饰、完美这座大厦了。”同时他也提到物理学的天空也飘浮着两朵小小的、令人不安的“乌云”：一朵为以太漂移实验的否定结果；另一朵为黑体辐射的紫外灾难。实际上“乌云”不止这两朵，还包括气体比热中能量均分定律的失败、光电效应实验、原子线光谱等。然而，就是这几朵“乌云”带来了一场震撼整个物理学界的革命风暴，导致了现代物理学的诞生。

1. 第一朵“乌云”以太学说

第一朵“乌云”是随着光的波动理论而开始出现的。菲涅耳和托马斯·杨研究过这个理论，它包括这样一个问题：地球如何通过本质上是光以太这样的弹性固体而运动呢？第二朵“乌云”是麦克斯韦-玻耳兹曼关于能量均分的学说。

这两朵“乌云”涉及两方面的实验发现与力学、电磁学、气体分子运动论理论。相对性原理是经典力学的一个最基本的原理，这个原理认为，绝对静止和绝对匀速运动都是不存在的，一切可测量的、有物理意义的运动，都是相对于某一参照物的相对运动。

牛顿本人也充分意识到确定“绝对运动”的困难，最后只能以臆测性的“绝对空间”的存在作为避难所。麦克斯韦的电磁场理论获得成功之后，电磁波的载体以太，就成了物化的绝对空间，静止于宇宙中的以太就构成了一切物体的“绝对运动”的背景框架。

既然以太也是一种物质存在，或者说它表征着物化了的绝对空间，当然就可以通过精密的实验测出物体相对于以太背景的绝对运动。但是，美国物理学家迈克尔逊在1881年、他和莫雷在1887年利用干涉仪所进行的精密光学实验，都未能观察到所预期的以太相对于地球的运动。

2. 第二朵“乌云”紫外灾难

第二朵“乌云”涉及的是经典物理学另一分支，是热力学和分子运动论中的一个重要问题。开尔文明确提到的是“麦克斯韦-玻耳兹曼关于能量均分的学说”。实际上是指19世纪末关于黑体辐射研究中所遇到的严重困难。

为了解释黑体辐射实验的结果，物理学家瑞利和金斯认为能量是一种连续变化的物

理量，建立起在波长比较长、温度比较高的时候和实验事实比较符合的黑体辐射公式。但是，这个公式推出，在短波区（紫外光区）随着波长的变短，辐射强度可以无止境地增加，这和实验数据相差十万八千里，是根本不可能的。

所以，这个失败被埃伦菲斯特称为紫外灾难。20 世纪初的这两朵“乌云”最终导致了物理学的一场大变革。

事隔不到一年，就从第一朵“乌云”中降生了相对论，紧接着从第二朵“乌云”中降生了量子论。经典物理学的大厦被彻底动摇。事实上，在 19 世纪末，光电效应、原子光谱和原子的稳定性等实验事实也接二连三地和经典物理学的理论发生了尖锐的对立。量子论的建立，使人类对物质的认识由宏观世界进入微观世界。

3.1.3 经典物理学的完成和局限

大约到了 1895 年前后，以经典力学、经典热力学和统计力学、经典电动力学为三大支柱的经典物理学，结合成一座具有雄伟的建筑体系和动人心弦的“美丽殿堂”，达到了它的巅峰时期。

1. 经典力学和机械决定论

由牛顿把它概括在一个严密的统一理论中，实现了近代物理学发展史上第一次理论大综合。在 1687 年出版的《自然哲学的数学原理》中，牛顿提出了动力学的三个基本原理和万有引力定律。利用变分法的数学方法和“最小作用量原理”的物理学基础建立起了和牛顿动力学方程等价的欧拉-拉格朗日方程，并最终于 1834 年由英国的哈密顿（1805—1865）提出了哈密顿原理和正则方程，建立了“分析力学”理论，实现了牛顿后力学理论的一个最大的飞跃。

2. 热力学与能量和熵

能量守恒原理的建立，使物理学思想和理论结构获得了辉煌的进展，是 19 世纪自然科学上的一个伟大胜利，也是近代物理学发展中的第二次理论大综合。熵原理的发现，实际上把演化的思想带进了物理学，指出了自然过程的不可逆性和历史性。

在经典力学和电磁场理论中，基本物理定律中的时间都是对称的、可逆的，它们的基

本方程对时间反演都是具有对称性的，运动对于过去和未来没有本质的区别，时间在那里仅仅是从外部描述运动的一个参量，它的变化对运动的性质并无影响。因而时间箭头在那里没有实质性的意义。

“统计力学”这个名称是1884年由美国物理学家吉布斯首先提出的。吉布斯在麦克斯韦和玻耳兹曼思想的基础上，明确形成了“系综”概念，创立了系综统计方法。从而将热学的唯象热力学和分子运动论的两个基本的研究方向统一到一个有机整体之中，完成了统计力学这个经典物理学的又一次理论大综合。

3.经典电动力学

1862年，麦克斯韦引入了一个电磁以太的准力学模型和“位移电流”假设，1864年提出了电动力学方程组，预言了电磁波的存在，并揭示了光的电磁波动本性。麦克斯韦的方案使媒介接触和传递的观念得以完全实现，并使电磁学理论的全部物理基础得以奠定，成为近代物理学发展中的第三次理论大综合。

4.经典物理学的完成和局限

(1) 在力学方面，与机械观相联系的绝对时间、绝对空间的概念以及关于质量的定义，都已受到普遍的批评，牛顿对于引力的本质问题也采取了回避的态度。而牛顿力学的理论框架实际上必然要把引力看作一种瞬时传递的超距作用，这与19世纪发展起来的场物理学是根本对立的。

(2) 在热学方面，熵增加原理揭示的与热现象有关的自然过程的不可逆性，反映出热力学原理与经典力学和经典电动力学原理之间深刻的内在矛盾，而统计力学中引入的概率统计思想以及热力学规律的统计性质，已使经典力学的严格确定性出现了缺口。

(3) 在光学和电磁学方面，作为光波与电磁波的传播媒介的“以太”，其令人难以理解的特殊性质以及关于它的存在的检测，都使科学家们费尽心血而一筹莫展。根据电磁学理论，用空间坐标的连续函数描写的场，具有能量的不能再简化的物理实在，这又与经典力学把运动的质点看作能量的唯一载体的观点背离。

牛顿在前人研究的基础上，取得了非凡的成就。运动三定律和万有引力定律成功地描述了天上行星、卫星、彗星的运动，又完满地解释了地上潮汐和其他物体的运动。此后

人们认为自然界的一切已知运动都可以通过牛顿（经典）力学定律解释。因此，牛顿（经典）力学被看作科学解释的最高权威和最后标准。

而经典力学建立的过程，实质上就是实验方法、逻辑思维方法与数学方法的建立和发展的过程。由此可以看出经典物理学中“经典”的含义。由著名的物理学家提出，经过反复的实验验证，最后得出最具权威最为标准最为经典的结论。

3.1.4　量子论的出现

量子力学是描述物质微观世界结构、运动与变化规律的物理科学。它是20世纪人类文明发展的一个重大飞跃，量子力学的发现引发了一系列划时代的科学发现与技术发明，对人类社会的进步做出重要贡献。

1. 经典理论无法解释的现象导致了量子论的出现

19世纪末正当人们为经典物理取得重大成就的时候，一系列经典理论无法解释的现象一个接一个地发现了。

爱因斯坦于1905年提出光量子说。1916年，美国物理学家密立根发表了光电效应实验结果，验证了爱因斯坦的光量子说。

1913年，丹麦物理学家玻尔为解决卢瑟福原子行星模型的不稳定性（按经典理论，原子中电子绕原子核做圆周运动要辐射能量，导致轨道半径缩小直到跌落进原子核），提出定态假设：原子中的电子并不像行星一样可在任意经典力学的轨道上运转，稳定轨道的作用量 fpdq 必须为 h 的整数倍（角动量量子化），即 $\mathrm{fpdq}=nh$，n 称为量子数。

玻尔原子理论以它简单明晰的图像解释了氢原子分立光谱线，并以电子轨道态直观地解释了化学元素周期表，导致了72号元素铪的发现，在随后的短短十多年内引发了一系列的重大科学进展。这在物理学史上是空前的。

由于量子论的深刻内涵，以玻尔为代表的哥本哈根学派对此进行了深入的研究，他们对对应原理、矩阵力学、不相容原理、测不准关系、互补原理、量子力学的概率解释等都做出了贡献。

1924年，美籍奥地利物理学家泡利发表了“不相容原理”：原子中不能有两个电子同

时处于同一量子态。这一原理解释了原子中电子的壳层结构。这个原理对所有实体物质的基本粒子(通常称为费米子,如质子、中子、夸克等)都适用,构成了量子统计力学——费米统计的基点。

1925 年,德国物理学家海森伯和玻尔,建立了量子理论的第一个数学描述——矩阵力学。1926 年,奥地利科学家提出了描述物质波连续时空演化的偏微分方程——薛定谔方程,给出了量子论的另一个数学描述——波动力学。1948 年,费曼创立了量子力学的路径积分形式。

以上研究成果都表明,光不仅仅是电磁波,也是一种具有能量动量的粒子。

量子力学在高速、微观的现象范围内具有普遍适用的意义。它是现代物理学的基础之一,在现代科学技术中的表面物理、半导体物理、凝聚态物理、粒子物理、低温超导物理、量子化学以及分子生物学等学科的发展中,都有重要的理论意义。量子力学的产生和发展标志着人类认识自然实现了从宏观世界向微观世界的重大飞跃。

2.与经典物理学的界限

1923 年,玻尔提出了对应原理,认为量子数(尤其是粒子数)高到一定的极限后的量子系统,可以很精确地被经典理论描述。这个原理的背景是,事实上,许多宏观系统,可以非常精确地被经典理论(如经典力学和电磁学)来描写。因此,一般认为在非常“大”的系统中,量子力学的特性,会逐渐退化到经典物理的特性,两者并不相抵触。

因此,对应原理是建立一个有效的量子力学模型的重要辅助工具。量子力学的数学基础是非常广泛的,它仅要求状态空间是希尔伯特空间,其可观察量是线性的算符。

但是,它并没有规定在实际情况下,哪一种希尔伯特空间、哪些算符应该被选择。因此,在实际情况下,必须选择相应的希尔伯特空间和算符描写一个特定的量子系统。对应原理是做出这个选择的一个重要辅助工具。

对应原理要求量子力学所做出的预言,在越来越大的系统中,逐渐近似经典理论的预言。这个大系统的极限,被称为“经典极限”或者“对应极限”。因此,可以使用启发法的手段,建立一个量子力学的模型,而这个模型的极限,就是相应的经典物理学的模型。

3.2　家族长子：牛顿力学

3.2.1　苹果为什么会落在牛顿头上

苹果当然不只落在了牛顿头上，它还落在了许许多多人的头上，但其他人都没有据此研究出什么定律，所以历史也就没有必要记载苹果还落在其他什么人头上了，因为没有什么意义。

当我们还是小学生的时候，老师在课堂里会讲到苹果如何落在牛顿头上，并给他带来灵感发现地心引力的故事，如图3-1所示。如果你态度不够谦卑，对这个故事提出质疑，那么你会发现教鞭会落在你的头上，这可不是什么地心引力。

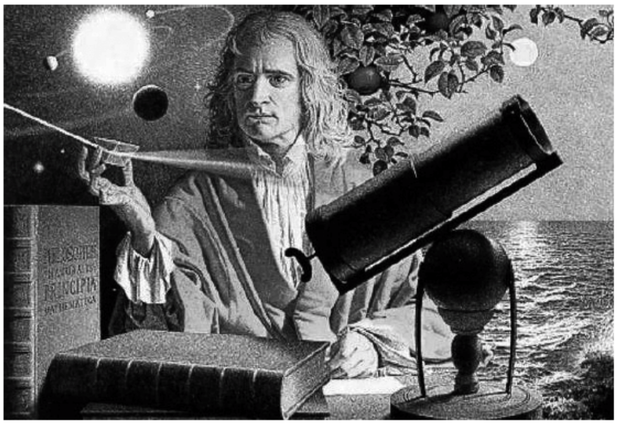


图3-1　苹果为什么会落在牛顿头上

苹果落在牛顿头上，其实只是个美丽的误会！

真有苹果砸中牛顿的故事吗？1665年到1666年，牛顿为了躲避在剑桥流行的瘟疫，回到了自己的家乡威尔索普，并经常在自家的花园里沉思。牛顿的传记作家韦斯特福尔表示：牛顿的侄女康杜伊特夫人曾说，当牛顿在花园中进行思考时，他突然想到，让苹果落地的地心引力并不限于地球，它能够在更大的范围内发生作用。也就是说，他早已经确信重力的存在了。当时他在考虑的问题不是苹果为何下落，而是重力是否能外推到月球

这样地外的物体。

事实上,18 世纪没有一个作家提到过牛顿被苹果砸中的故事。韦斯特福尔表示,“苹果的故事让人误以为当时的人们对地心引力一无所知”,而科学家迈克尔·怀特则说,“苹果的故事几乎肯定是虚构的。”

那为什么“苹果砸牛顿”的故事如此深入人心呢?让我们回到行为经济学来回答这个问题。

当第一次得知地心引力的时候,我们的教育便和那只看不见的苹果牢牢地捆绑在一起了。这就相当于“锚定效应”,所谓锚定,就是通过第一印象产生偏见的一种心理的偏向。

人们通常做出各种判断是依据记忆中最易于使用的信息。也就是说,信息越容易记,就越倾向于作为判断的依据(可用性启发法)。地心引力和苹果,如同“送礼”和“脑白金”被千百遍地黏合在了一起,这个神话也就越来越广地传播。

这样的故事很多。年轻的华盛顿为了试自己的新斧子而砍断了父亲的樱桃树,华盛顿大义凛然地说:“爸爸,我不能说谎,是我砍断了樱桃树。”事实上这个故事本身就是一个谎言。《大英百科全书》告诉我们,这句话实际上是美国牧师和旅行书商帕森·威姆斯瞎编的。

瓦特的婶婶对瓦特说:“瓦特,我从未见过像你一样懒惰的男孩,去看书或者找点事情吧;整整一个小时中,你做的就是把壶盖拿开和放回原处,把杯子和银勺放在蒸汽上,看蒸汽把它们推开以及观察一滴滴热水。你难道不觉得羞耻吗?”然而瓦特对茶壶的蒸汽着了迷,因此发明了蒸汽机。这个故事也很鲜活,但事实上瓦特是 1736 年诞生的,第一台蒸汽机是托马斯·纽科门于 1712 年在斯塔福德建造的。

诺贝尔经济学奖得主丹尼尔·卡尼曼说,“好的故事为人们的行为和意图提供了简单且合乎逻辑的解释。引人入胜的故事会使人产生某种必然性错觉。”18 世纪的作家和哲人(其中包括伏尔泰)开始大肆宣扬牛顿和苹果的故事,就是为了用通俗的科学故事启发民众,即便今天也是如此。

“有一天,一个苹果落到了牛顿头上……”这个故事还会一直讲下去。

3.2.2 牛顿是谁

牛顿于1643年1月4日生于英格兰林肯郡格兰瑟姆附近的威尔索普村。1661年入英国剑桥大学三一学院，1665年获文学学士学位。1667年，牛顿回剑桥后当选为剑桥大学三一学院院委，次年获硕士学位。1669年，任剑桥大学卢卡斯数学教授席位直到1701年。1703年，任英国皇家学会会长。1706年，牛顿受英国女王安娜封爵。1727年，牛顿在伦敦病逝，享年84岁。牛顿肖像如图3-2所示。

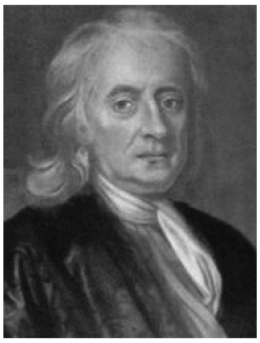


图3-2 牛顿

1. 牛顿力学由来

牛顿力学是以牛顿运动定律为基础，在17世纪以后发展起来的。直接以牛顿运动定律为出发点来研究质点系统的运动，就是牛顿力学。

牛顿试图使用惯性与力的概念描述所有物体的运动，所以他找寻出它们服从确定的守恒定律。1687年，牛顿接着出版了他的自然哲学的数学原理论文。在这里牛顿开创了三个运动定律，到了今日还是描述力的方式。

2. 牛顿力学定律

牛顿力学涉及很多方面，它们都涉及最基本的三个定律。

1）牛顿第一定律

内容：一切物体在没有受到力或合力为零的作用时，总保持静止状态或匀速直线运动状态。

说明：物体都有维持静止和做匀速直线运动的趋势，因此，物体的运动状态是由它的运动速度决定的，没有外力，它的运动状态是不会改变的。物体的这种性质称为惯性。所以牛顿第一定律也称为惯性定律。第一定律明确了力是物体间的相互作用，指出了是力改变了物体的运动状态。因为加速度是描写物体运动状态的变化，所以力是和加速度相联系的，而不是和速度相联系的。在日常生活中不注意这点，往往容易产生错觉。

注意：牛顿第一定律并不是在所有的参照系里都成立，实际上它只在惯性参照系里

才成立。因此，常常把牛顿第一定律是否成立，作为一个参照系是否是惯性参照系的判据。

2）牛顿第二定律

内容：物体受到合外力的作用时会产生加速度，加速度的方向和合外力的方向相同，加速度的大小与合外力的大小成正比，与物体的惯性质量成反比。

公式：$F=ma$，F 为合外力。

牛顿第二定律定量描述了力作用的效果，定量地度量了物体的惯性大小。它是矢量式，并且是瞬时关系。

要强调的是，物体受到的不为零合外力，会产生加速度，使物体的运动状态或速度发生改变，但是这种改变是和物体本身的运动状态有关的。

局限：该定律只适用于宏观物体的低速运动。

3）牛顿第三定律

内容：两个物体之间的作用力和反作用力，在同一条直线上，大小相等，方向相反。

需要注意：

(1) 作用力和反作用力没有主次、先后之分，同时产生、同时消失。

(2) 这一对力是作用在不同物体上，不可能抵消。

(3) 作用力和反作用力必须是同一性质的力。

(4) 与参照系无关。

3.牛顿力学定义

牛顿力学以牛顿运动定律和万有引力定律（见万有引力）为基础，研究速度远小于光速的宏观物体的运动规律。

狭义相对论研究速度能与光速比拟的物体的运动，量子力学研究电子、质子等微观粒子的运动。

从研究的范畴来说，牛顿力学是经典力学的组成部分。继牛顿以后，拉格朗日和哈密顿相继发展了新的力学体系。

牛顿力学所着重的量如力、动量等都具有矢量性质，而且牛顿方程是用矢量形式表达

的，故牛顿力学可称为矢量力学。

拉格朗日体系和哈密顿体系所着重的量是系统的能，它具有标量的性质，可以通过力学的变分原理建立系统的动力学方程，故拉格朗日体系和哈密顿体系等可统称为分析力学。

因此，从力学的研究方法和体系来说，牛顿力学同拉格朗日体系和哈密顿体系相互有区别；但从经典力学的基本原理来说，拉格朗日方程和哈密顿原理同牛顿定律是等价的。

3.2.3　牛顿想的也对也不对：适用范围与局限性

1. 开辟新时代

17 世纪的欧洲，经过许多科学家的努力，在天文学和力学方面积累了丰富资料的基础上，英国科学家牛顿实现了天上力学和地上力学的综合，形成统一的力学体系——经典力学。经典力学体系的建立，是人类认识自然及历史的第一次大飞跃和理论的大综合，它开辟了一个新的时代，并对科学发展的进程以及人类生产生活和思维方式产生极其深刻的影响。牛顿经典力学的建立是科学形态上的重要变革，标志着近代理论自然科学的诞生，并成为其他各门自然科学的典范。

2. 条件和原因

牛顿经典力学体系的建立得益于已有的科学成就。哥白尼、伽利略、开普勒、笛卡儿等人在天文学、力学、光学、数学等方面的贡献，为经典力学奠定了坚实的基础，特别是伽利略与开普勒对牛顿经典力学体系的建立更是有着极其重要的影响。

伽利略通过对自由落体的研究，发现了惯性运动和在重力作用下的匀加速运动，奠定了牛顿第一定律和第二定律的基本思想。伽利略关于抛物体运动定律的发现，对牛顿万有引力的学说也有深刻的启示作用。开普勒所发现的行星运动定律则是牛顿万有引力学说产生的最重要前提。牛顿非常善于广泛汲取前人的科学成果并综合运用多方面的知识进行跨学科的研究，通过吸收前人的科学研究成果，牛顿为经典力学体系的建立充实了知识准备。

虽然经典力学建立在丰富的科学经验之上，但经典力学的建立和牛顿的个人原因有

不可分割的关系。牛顿从青少年时代就对科学抱有浓厚的兴趣、极强的求知欲和探索欲望，学习非常勤奋。但他从不死读书，喜欢通过实验来取得真知，并亲自动手设计和制作了许多机械装置和用品，这使他打下了广博而扎实的知识基础，同时也具有创新意识和动手能力。

牛顿经典力学的建立，还与他所处的时代和社会有关。欧洲经过16世纪百余年的宗教和政治改革的大变动之后，到17世纪下半叶进入了一个政治上转为安宁，经济上趋于繁荣的时期。生产实践为力学研究提出了许多问题，这就给科学的发展以推动力。经过16世纪的宗教改革运动和17世纪中后期的资产阶级革命运动，英国科学家拥有了当时世界上最为宽松自由的学术环境。学术环境的改变，使得对力学的研究摆脱了不必要的束缚，催生了经典力学体系。

个人因素，前人经验，宽松的学术环境和生产实践的发展，构成了经典力学体系建立的条件和基础。

3.经典力学影响

不难预料，经典力学的巨大成功对人类社会在各方面产生不可估量的影响。

1）对自然观念的影响

牛顿经典力学的成就之大使得它得以广泛传播，深深地改变了人们的自然观。人们往往用力学的尺度去衡量一切，用力学的原理去解释一切自然现象，将一切运动都归结为机械运动，一切运动的原因都归结为力，自然界是一架按照力学规律运动着的机器。这种机械唯物主义自然观在当时是有进步作用的。

由于它把自然界中起作用的原因都归结为自然界本身规律的作用，有利于促使科学家去探索自然界的规律。它能刺激人们运用分析和解剖的方式，从观察和实验中取得更多的经验材料，这对科学的发展来说也是必要的。但这种思维方式在一定程度上忽视了理论思维的作用，忽视了事物之间的联系和发展，因而又有着严重的缺陷。

2）对自然科学的影响

牛顿经典力学的内容和研究方法对自然科学，特别是物理学起了重大的推动作用，但也存在着消极影响。

牛顿建立的经典力学体系以及他的力学研究纲领所获得的成功，在当时使科学家们以为牛顿经典力学就是整个物理学，甚至是全部自然科学的可靠的最终的基础。在相当长的历史时期内，牛顿经典力学名著《自然哲学的数学原理》一书成为了科学家们共同遵循的规范，它支配了当时整个自然科学发展的进程。

他研究问题的科学方法和原理也普遍得到赞赏和采用。牛顿研究经典力学的科学方法论和认识论，如运用分析和综合相结合的方法与公理化方法及科学的简单性原则、寻求因果关系中的相似性统一性原则、以实验为基础发现物体的普遍性原则和正确对待归纳结论的原则，对后世科学的发展影响深远。

3）牛顿力学对社会科学的影响

经典力学不但对自然科学产生了很大影响，在社会科学方面，特别是对哲学和人类思想的发展，也产生了重大影响。

在经典力学的直接影响下，英国的霍布斯和洛克建立并发展了机械唯物主义哲学。由于其强大的影响力，使得唯物论从宗教神学那里争得了发言权，并在随后形成了人类历史上唯物主义和唯心主义斗争最为激烈的一段时期。

经过康德和黑格尔对辩证法和机械唯物主义的研究和发展，以及马克思和恩格斯对哲学已有研究成果的吸收，结合当时科学发展成果，最终建立了唯物主义辩证法。唯物主义辩证法的建立，在很大程度上得益于牛顿经典力学体系的建立。

近现代科学和哲学发轫于经典力学，正是从牛顿建立经典力学开始，人类在思想观念上才开始真正走向科学化和现代化，而它对人类思想领域的影响也是极其广泛而深刻的。

4.牛顿力学的得与失

事物总是辩证统一、一分为二的。虽然科学家在运用牛顿经典力学方法及成果时使自然科学得到了长足发展，但当时人们在接受和运用牛顿的科学成果之时，没有搞清它的适用范围，也做出了不适当的夸大。

例如，当初有科学家认为所有涉及的物理学问题都可以归结为不变的引力和斥力，因而只要把自然现象转化为力就行了。结果到后来，“力”成了对现象和规律缺乏认识的避难所，把当时无法解释的各种现象都冠以各种不同力的名称。因此，牛顿经典力学的内容

及其研究方法在推动自然科学发展的同时，也产生了很大的消极影响。

1）牛顿力学的伟大成就

经典力学把人类对整个自然界的认识推进到一个新水平，牛顿把天上运动和地上运动统一起来，从力学上证明了自然界的统一性，这是人类认识自然历史的第一次大飞跃和理论大综合，它开辟了一个新时代，并对学科发展的进程以及后代科学家们产生了极其深刻的影响。

经典力学的建立首次明确了一切自然科学理论应有的基本特征，这标志着近代理论自然科学的诞生，也成为其他各门自然科学的典范。牛顿运用归纳与演绎、综合与分析的方法极其明晰地得出了完善的力学体系，被后人称为科学美的典范，显示出物理学家在研究物理时，都倾向于选择和谐与自洽的体系，追求最简洁、最理想的形式。

经典力学的建立对自然科学和科技的发展、社会进步具有深远影响。一是科学的研究方法推广应用到物理学的各个分支学科上，对经典物理学的建立意义重大；二是经典力学与其他基础科学相结合产生了许多交叉学科，促进了自然科学的进一步发展；三是经典力学在科学技术上有广泛的应用，促进了社会文明的发展。

2）牛顿力学适用范围及其局限性

经典力学的应用受到物体运动速率的限制，当物体运动的速率接近真空中的光速时，经典力学的许多观念将发生重大变化。例如，经典力学中认为物体的质量不仅不变，并且与物体的速度或能量无关，但相对论研究表明，物体的质量将随着运动速率的增加而增大，物体的质量和能量之间存在密切的联系。但当物体运动的速度远小于真空中的光速时，经典力学仍然适用。

牛顿运动定律不适用于微观领域中物质结构和能量不连续现象。19世纪末和20世纪初，物理学的三大发现，即X射线的发现、电子的发现和放射性的发现，使物理学的研究由宏观领域进入微观领域，特别是20世纪初量子力学的建立，出现了与经典力学不同的新观念。

例如，量子力学的研究表明，微观粒子既表现为粒子性又表现为波动性，粒子的能量等物理量只能取分立的数值，粒子的速度和位置具有不确定性，粒子的状态只能用粒子在

空间出现的概率来描述等。但量子力学的建立并不是对经典力学的否定，对于宏观物体的运动，量子现象并不显著，经典力学依然适用。

现代物理学的发展，并没有使经典力学失去存在的价值，只是拓宽了人们的视野，经典力学仍将在它适用的范围内大放异彩。

3.3　家族长孙：量子力学

先简单解释一下量子力学的内容。请诸位做好准备，下面这一段可能一时看不懂！没关系，95％的读者和你一样都不太懂，把这本书坚持看完你就懂了。就像你上小学一年级碰到的巨难的题，等你升到二年级回头一看就豁然开朗了。

量子力学的核心概念是波函数。给定系统的波函数就能够完整描述该系统的运动状态，即描述该系统的全部可测量的物理量的具体情况，亦即该系统的能量、动量、角动量、位置等物理量到底是多少乃至它们怎样随时间而变。

当然，一般来说，波函数只能说出系统的某个物理量为某个具体数值的概率有多大（即多次同样的测量所得到的该数值的占比是多少），而不能说出该系统的物理量一定等于某个值，除非该系统对于该物理量存在本征态及相应的本征值。

量子力学的基本假设（或原理或公式，它们本质上都是需要经实践检验的假设）包括态（波函数）叠加原理、波函数的统计诠释、测不准原理、观测量的算符化、测量的投影假设（即波包缩编、波函数坍缩等）、运动方程（如薛定谔方程）。这些假设都是为了具体计算波函数并将它与实验数据相比较而创立的，其间涉及大量的数学推演。

经典的哈密顿方程，通过力学量算符化改造，就能变成量子力学的方程；总之，在形式上，经典方程与量子方程有一脉相承的关系，但在对方程的各个要素的物理诠释上，两者相差很大。可以说，量子力学是以一种全新的方式在描述自然的运作。

3.3.1　量子力学漫谈

20世纪有两大发现：相对论和量子力学。量子力学和爱因斯坦的相对论是同一个时

代的成果，但却和相对论的一些理论相悖。爱因斯坦一直推崇这个宇宙的所有物理现象都是可测量的，可以用确定的语言描述的，他称之为大理石般的宇宙，但量子力学的研究打破了他的理想。

1. 量子力学所要表明的事实

量子力学所要表明的事实就是，当人类所研究的物质到了基本粒子这一层次，有可能因为测量工具的干扰而导致得出的结果不同。所以说，在这个层次上，好像因为人的观测行为，而导致了物质的不确定性。如果你不去观测，你就没办法确定这个物质的状态。

上升到宏观物质的层次，所有的物质的都是由基本粒子所组成，它们都具有量子态。所以，很有可能处于像薛定谔猫的那种半死不活状态，但由于人的观测无所不在，在宏观情况下，量子态一直处于确定的状态，所以不会出现可怕的情形。

这也是爱因斯坦最不理解的地方，物质怎么可能既存在又不存在，而要依赖于人的观测？似乎有点唯心了。

但很多实验都证实了量子力学的事实，例如，那个有名的ERP佯谬。这个是老爱试图对量子力学证伪的一个假设，即当1个粒子分成2半，然后一个向左一个向右，那么，当你观测其中的一半，另一半必定也会处于相同的状态，无论相隔多远。也就是说，如果一半是在向左旋转，那另一半就会向右旋转，反之亦然。后来的实验证实了这个情况。

量子力学是个统计科学，这是因为它强调的不是确定的数值，只是统计的概率。例如，这个粒子，在我们观测前，我们不能得知它会在哪里，但我们可以计算出它大概在哪里，它出现的位置可以通过统计它的所出现位置的概率来得出。

简单地说，量子力学研究的是原子、分子、电子等组成宏观物质的微观粒子的运动规律和原理。例如，电子如何与原子核相互作用、作用的本质是什么、能够干什么、如何精确计算等。

2. 量子力学与其他物理学分支的最大区别

1）引入了完全的量子论

量子力学与其他物理学分支的最大区别就是引入了完全的量子论。量子论不是一个具体的理论，而是一种有别于经典物理学的新思想。它强调世界不是连续的，具体一点就

是物质、能量、运动过程、时间都不能无限细分，它们都有不可分割的最小单位。

例如，时间的最小单位是普朗克时间，相邻的2个普朗克时间之间不可以再分割，否则没有任何意义。物质、能量、运动过程都有类似的不可无限分割的性质。

例如，一个电子在A、B两个不相邻的微观区域中运动，那么这个电子从区域A运动到区域B可以不经过A、B中间的任何地方，即电子瞬间从区域A“变”到了区域B。

粒子可以瞬移、凭空出现、无缘无故消失等，这些就是奇怪的量子效应。犹如“现在流通的人民币面值是不能无限分割的，它的最小单位是1分”，这也属于量子论。

量子论完全应用于力学研究就产生了量子力学。众所周知，微积分的基础就是无限分割（准确地说是微分学），量子论无疑冲击了微积分这一高等数学基础理论在物理学研究中的权威地位。

2）另外一个理论是不确定性

量子论的另外一个理论是不确定性，它由著名的不确定性关系作为坚实的后盾（爱因斯坦质疑过这个理论的可靠性，但是被玻尔驳倒了）。

经典物理学有宿命论这个论调，虽然没有人正式提出，但是很多人都相信：既然万事万物的运动过程都可以用物理方程描述，那么这个宇宙从诞生开始就已决定了最终的结局，所有的现象都只是物质机械的物理运动，即宇宙与每个人的命运都注定了，不可更改；人类只是计算能力有限，只要条件许可，我们可以预测一切未来。

因为万物都符合物理原理，而终极物理原理是相当确定的（人类目前还没能达到，但不等于达不到），它就是真理，操纵这个世界的运作。条件一定，一个数学方程不可能有多解。同理，当真理数字方程化以后，世界的发展方向也就唯一了。

量子论给了机械主义的宿命论狠狠的一巴掌。量子论指出：世界一切皆有可能，宏观的物理理论不再适用于微观领域，未来发生某事只能用概率大小描述，没有严格的必然事件；过去与未来一样，也可以改变；时间不一定要按照过去→现在→未来的方向流动；历史或者宇宙其实不止一个……最重要的是，上帝不喜欢确定性，上帝是玩骰子的。

3）量子力学用数学描述研究微观粒子可能的运动

量子力学主要还是研究微观领域的数学描述，使用一些繁杂的微分方程式计算微观

粒子可能的运动情况，对哲学问题尽量回避不谈，因为量子论的原理比相对论还难，以至于世界上没有一个科学家可以完全理解。科学家们现在只关心某个方程能不能产生实际作用，能不能对结果做出较精确的计算和预测。对于一些方法为什么可行，为什么可以算出正确答案，他们就不管了。

3.3.2 量子力学是用来解释微观粒子的物理分支

原子、分子、电子等微观粒子用宏观世界的牛顿力学无法解释，例如电子围绕原子核转动。用牛顿力学来看，电子受到原子核的引力要等于它旋转产生的离心力，离心力大小与旋转半径和转速有关。按照这个理论只要电子旋转速度改变，电子的旋转半径也就是离原子核的距离就会改变。而实际上不是这样，电子运行速度没有改变，它运行的轨道也会变化，这用牛顿力学是无法解释的。

这时候就要靠量子力学的轨道能量来解释，电子获得外部能量就会向高能量的轨道跃迁。简单一点就是，你能看到的世界都是符合三大牛顿运动定律的，而看不见的微观世界，涉及原子、分子、光波等牛顿定律不可用，要研究它们就要使用量子力学里面的定律。

如果用一句话描述量子力学的内容，你一定要谨记这个底线：**牛顿力学讲的是确定，量子力学讲的是不确定**。

量子力学是研究微观粒子的运动规律的物理学分支学科，它主要研究原子、分子、凝聚态物质，以及原子核和基本粒子的结构、性质的基础理论，它与相对论一起构成现代物理学的理论基础。量子力学不仅是近代物理学的基础理论之一，而且在化学等有关学科和许多近代技术中也得到了广泛的应用。

简单地说，量子力学讲的是小到肉眼看不见，同时又快到肉眼看不见的那些小粒子们的事儿。它们很神奇，你知道它们位置，就不知道它们的速度；知道它们的速度，就不知道它们的位置（测不准原理）。你不看它们的时候，它们是一个样；你观察它们的时候，它们马上又变成另外一个样。所以，人们永远不知道它原本是什么样的（薛定谔的猫理论）。

对于量子力学没基础的人，可以理解的概念有以下几个。

1. 波粒二象性

波粒二象性（wave-particle duality）指的是所有的粒子或量子不仅可以部分地以粒子

的术语来描述，也可以部分地用波的术语来描述。这意味着经典的有关“粒子”与“波”的概念失去了完全描述量子范围内的物理行为的能力。

爱因斯坦这样描述这一现象：“好像有时我们必须用一套理论，有时又必须用另一套理论来描述(这些粒子的行为)，有时又必须两者都用。我们遇到了一类新的困难，这种困难迫使我们要借助两种互相矛盾的观点来描述现实，两种观点单独是无法完全解释光的现象的，但是合在一起便可以。”

波粒二象性是微观粒子的基本属性之一。1905年，爱因斯坦提出了光电效应的光量子解释，人们开始意识到光波同时具有波和粒子的双重性质。1924年，德布罗意提出“物质波”假说，认为与光一样，一切物质都具有波粒二象性。根据这一假说，电子也具有干涉和衍射等波动现象，这被后来的电子衍射实验所证实。

2015年，瑞士洛桑联邦理工学院的科学家成功拍摄出光同时表现波粒二象性的照片，如图3-3所示。

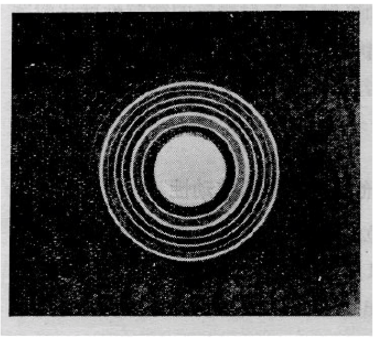


图3-3　光同时表现波粒二象性的照片

2. 海森伯不确定性原理

物理学家认为不确定性原理(uncertainty principle)是由海森伯于1927年提出。当时德国物理学家海森伯发现，经典物理学对极小的物体(即单个原子级别)并不适用。例如，如果把一个球抛向空中，很容易判断球的所处位置和运动速度。但海森伯指出，对原子和亚原子粒子而言，这是行不通的。观察者要么只能看到它的位置，要么只能判断它的运动速度，但无法同时获得两项信息。

这个理论是说，人们不可能同时知道一个粒子的位置和它的速度，粒子位置的不确定性，必然大于或等于普朗克常数(Planck constant)除于4π($\Delta x\Delta p \geqslant h/4\pi$)，这表明微观世界的粒子行为与宏观物质很不一样。

此外，不确定原理涉及很多深刻的哲学问题，用海森伯自己的话说：“在因果律的陈述中，即‘若确切地知道现在，就能预见未来’，所得出的并不是结论，而是前提。我们不能

知道现在的所有细节，是一种原则性的事情。”

意识到这一点令人颇为不安。自从海森伯解释了这一概念，爱因斯坦和其他科学家就感到十分不快。要知道，这种“量子不确定性”并非由测量设备或工程缺陷导致，而是与人们大脑的运作方式有关。人们已经习惯了“经典世界”的运作规律，因此，“量子世界”的物理机制难免超出了人们的接受范围。

例如，极小的粒子有一定概率穿过势垒的事实，如图 3-4 所示。

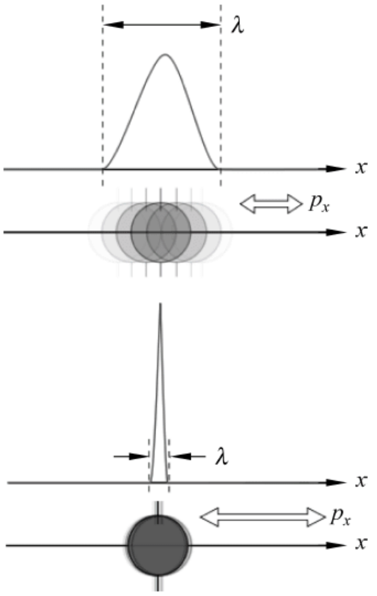


图 3-4　极小的粒子有一定概率穿过势垒

3.3.3　“薛定谔猫”的困境

薛定谔猫是奥地利著名物理学家薛定谔提出的一个思想实验，试图从宏观尺度阐述微观尺度的量子叠加原理的问题，巧妙地把微观物质在观测后是粒子还是波的存在形式与宏观的猫联系起来，以此求证观测介入时量子的存在形式。随着量子物理学的发展，薛定谔的猫还引申出平行宇宙等物理问题和哲学争议。

薛定谔的猫是关于量子理论的一个理想实验。实验内容：这只猫十分可怜，它被封在一个密室里，密室里有食物和毒药。毒药瓶上有一个锤子，锤子由一个电子开关控制，电子开关由放射性原子控制。

如果原子核衰变，则放出 α 粒子，触动电子开关，锤子落下，砸碎毒药瓶，释放出里面的氰化物气体，猫必死无疑。这个残忍的装置由奥地利物理学家薛定谔设计，所以此猫便称为薛定谔猫。

这个设备的开关是一个检测粒子放射性的装置（比如盖革计数器），这个装置旁边放个放射性物质，这个放射性物质既可能发生衰变，产生放射性，又可能不发生衰变，所以当你没打开箱子时，你无法确定这只猫是否还活着，所以它的状态是半死不活状态（应该说既是死的，又是活的），如图 3-5 所示。

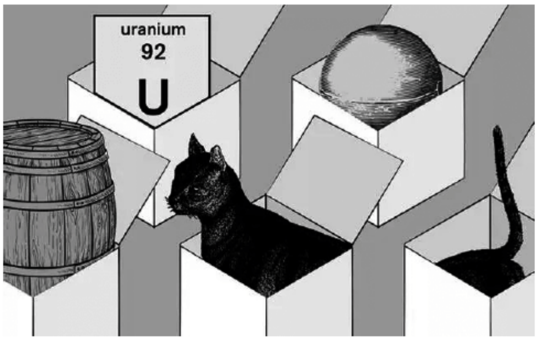


图 3-5　薛定谔那既生又死的猫

薛定谔打造这个思想实验，是在 1935 年夏天与爱因斯坦的一场对话中。之前，他们俩都对量子理论做出过巨大贡献，并为此获得诺贝尔奖。也许是受到与爱因斯坦近期交流的影响，薛定谔开始撰写他自己的长论文，题为《量子力学的现状》（*The Present Situation in Quantum Mechanics*）。

薛定谔写道：“密闭的铁匣子里放着一个盖革计数器和少量的铀，因为量非常少，所以很可能一个小时内有一个原子衰变的概率和没有衰变的概率一样。当第一次衰变发生时，通过继电器，装置会释放锤子砸碎一瓶氢氰酸。更残忍的是，还有一只猫被关在这个铁匣子里。”与爱因斯坦的例子一样，薛定谔假想预定的时间过后，根据量子力学的理论，此时既可以说猫是活的，又可以说猫是死的，如图 3-6 所示。

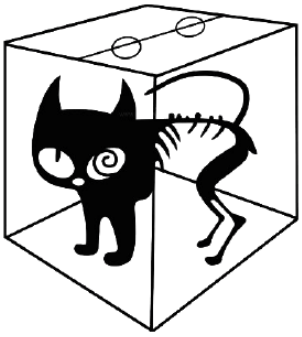


图 3-6　科学史上最著名的猫，以及它令人意外的残忍隐喻

多年之后，薛定谔臆想中将挫败量子力学的一个思想实验，却成为用来教授量子论的

经典比喻之一。量子力学的一个中心原则就是粒子可以存在于叠加态中，能同时拥有两个相反的特性。尽管我们在日常生活中常常面对“不是 A 就是 B”的抉择，而大自然（至少在量子论的描述中）是可以接受“既是 A 又是 B”的。

在过去的几十年里，物理学家成功地在实验室中实现了多种薛定谔猫态，将物质微粒转变为“既是 A 又是 B”的叠加态，并探测它们的性质。尽管薛定谔对此持保留意见，然而每一次测试结果都符合量子力学的理论预测。在实验中，科学研究人员证明了中微子（一种与普通物质相互作用非常微弱的亚原子）可以在薛定谔猫态下移动数百英里。

量子理论认为：如果没有揭开盖子，进行观察，我们永远也不知道猫是死是活，它将永远处于非死非活的叠加态，这与人们的日常经验严重相违。

3.3.4 量子世界中，波函数到底是数学描述还是实体

量子力学的发展已有百年历程，但身为其理论核心之一的波函数，其本质到底是什么，却依然是百年未解的谜团。波函数理论已经衍生出诸如激光、半导体和核能等高新技术，深刻地改变了人类的生活方式。但多年来，物理学家们提出各种关于波函数的假设和诠释，并设计出各种实验进行验证，却始终没有达成共识。其中最主流声音认为，波函数仅是一种数学描述，用来计算微观物体在某处出现的概率，如图 3-7 所示。

图 3-7　波函数是一种数学描述

有这样一个世界：崂山道士的穿墙术成为可能，你脚下的大地也不再坚实，甚至世界的客观实在性也消失了，一切都要用概率来解释。这就是量子力学的世界。

1. 双缝实验量子世界最早展示的怪事之一

英国物理学家托马斯·杨在1801年首次观察到了光的双缝干涉，一束光经过两条很窄的缝隙后产生了数条明暗条纹，屏幕上交替出现相长和相消干涉的区域。

光波是由大量的“光子”或者“光量子”组成的，在强光的情况下，光就是一束电磁波。因此，当一束光穿过两个缝隙时，在缝后会相互干涉，进而形成干涉条纹。

但是在这里，我们将看到物理学中最疯狂的实验结果之一。我们每次只发射一个光子，已排除了两个光子的相互影响。然而，在这种情况下，经过长时间的积累，干涉条纹依然会出现。每个光子到达屏幕时，只产生一个亮点。第一个光子在屏幕上一个特定位置被检测到，第二个、第三个以及第四个光子也一样，每一个光子都将在屏幕上产生一个亮点，表现出粒子的特性。如果不断发射单个光子，在发射足够多的单个光子后，这些光子在屏幕上就形成了干涉条纹的图案。

虽然我们不知道每个光子会落在屏幕上哪一点，也不知道下一个光子会落在哪儿，但是每个光子在落向屏幕时肯定是干涉条纹亮点的地方，不会落在干涉暗点的地方，这样最终呈现出干涉条纹。

光子并不是唯一这样做的粒子，发射单个电子穿过一对缝隙，它也会在屏幕上某一点处落下。发射许多电子后，会形成同样的干涉条纹，甚至用包含有几千个原子、电子、原子核组成的大分子做双狭缝实验，也能观察到这一奇怪现象。

此时，每个光子、电子或原子经过双狭缝时表现出波的干涉性质，这表现出微观粒子的波动性，而在屏幕上我们看到的只是一个亮点，又表现出粒子性。人们将微观粒子的这种既有波动性又有粒子性的奇妙性质，称为波粒二象性。

2. 波函数

波函数是量子力学中描写微观系统状态的函数。在经典力学中，用质点的位置和动量（或速度）来描写宏观质点的状态，这是质点状态的经典描述方式，它突出了质点的粒子性。由于微观粒子具有波粒二象性，粒子的位置和动量不能同时有确定值（见测不准关

系），因而质点状态的经典描述方式不适用于对微观粒子状态的描述，物质波在宏观尺度下表现为对概率波函数的期望值，不确定性失效可忽略不计。

在量子力学中，为了定量地描述微观粒子的状态，量子力学中引入了波函数，并用 Ψ 表示。一般来讲，波函数是空间和时间的函数，并且是复函数，即 $\Psi=\Psi(x,y,z,t)$。将爱因斯坦的“鬼场”和光子存在的概率之间的关系加以推广，玻恩假定 $\Psi^*\Psi$ 就是粒子的概率密度，即在时刻 t，在点 (x,y,z) 附近单位体积内发现粒子的概率。波函数 Ψ 的绝对值的平方称为概率幅。

图 3-8　电子双缝干涉实验

电子在屏上各个位置出现的概率密度并不是常数：有些地方出现的概率大，即出现干涉图样中的“亮条纹”；而有些地方出现的概率却可以为零，没有电子到达，显示“暗条纹”。电子双缝干涉实验如图 3-8 所示。

由此可见，在电子双缝干涉实验中观察到的，是大量事件所显示出来的一种概率分布，这正是玻恩对波函数物理意义的解释，即波函数模的平方对应于微观粒子在某处出现的概率密度（probability density），即微观粒子在各处出现的概率密度才具有明显的物理意义。

据此可以认为波函数所代表的是一种概率的波动。这虽然是人们对物质波所能做出的一种理解，但是波函数概念的形成正是量子力学完全摆脱经典观念、走向成熟的标志；波函数和概率密度是构成量子力学理论的最基本的概念。

3.3.5　搞量子力学没点高数基础不行——薛定谔方程

薛定谔方程又称为薛定谔波动方程，是 1926 年由奥地利物理学家薛定谔提出的量子力学中的一个基本方程，也是量子力学的一个基本假定。

薛定谔（1887—1961 年，见图 3-9）1887 年 8 月 12 日出生于奥地利首都维也纳；1906 年至 1910 年，他就读于维也纳大学物理系；1910 年获得博士学位；1921 年薛定谔受聘到瑞士的苏黎世大学任数学物理教授，在那里工作了 6 年，薛定谔方程就是在这一期间提

出的。

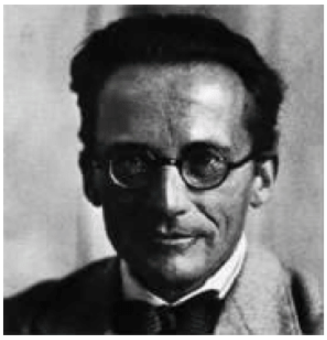


图 3-9 薛定谔

1927 年薛定谔接替普朗克到柏林大学担任理论物理教授。1933 年移居牛津，在马达伦学院任访问教授。1933 年他与狄拉克共同获得诺贝尔物理学奖。

薛定谔方程描述微观粒子的状态随时间变化的规律。微观系统的状态由波函数来描写，薛定谔方程即是波函数的微分方程。若给定了初始条件和边界条件，就可由此方程解出波函数。

薛定谔方程是将物质波的概念和波动方程相结合建立的二阶偏微分方程，可描述微观粒子的运动，每个微观系统都有一个相应的薛定谔方程式，通过解方程可得到波函数的具体形式以及对应的能量，从而了解微观系统的性质。薛定谔方程表明量子力学中，粒子以概率的方式出现，具有不确定性，宏观尺度下失效可忽略不计。

薛定谔方程的定义

在量子力学中，体系的状态不能用力学量（例如 x）的值来确定，而是要用力学量的函数 $\Psi(x,t)$，即波函数（又称为概率幅，态函数）来确定，因此，波函数成为量子力学研究的主要对象。力学量取值的概率分布如何，这个分布随时间如何变化，这些问题都可以通过求解波函数的薛定谔方程得到解答。这个方程是量子力学最基本的方程之一，在量子力学中的地位与牛顿方程在经典力学中的地位相当，超弦理论试图统一两种理论。

薛定谔方程是量子力学最基本的一个基本假定，其正确性只能靠实验来确定。

量子力学中求解粒子问题常归结为解薛定谔方程或定态薛定谔方程。薛定谔方程广泛地用于原子物理、核物理和固体物理，对于原子、分子、核、固体等一系列问题中求解的结果都与实际符合得很好。

薛定谔方程数学形式描述如下。

一维薛定谔方程：

$$-\frac{\hbar^2}{2\mu}\frac{\partial^2\Psi(x,t)}{\partial x^2}+U(x,t)\Psi(x,t)=i\hbar\frac{\partial\Psi(x,t)}{\partial t}$$

三维薛定谔方程：

$$-\frac{\hbar^2}{2\mu}\left(\frac{\partial^2\Psi}{\partial x^2}+\frac{\partial^2\Psi}{\partial y^2}+\frac{\partial^2\Psi}{\partial z^2}\right)+U(x,y,z)\Psi=i\hbar\frac{\partial\Psi}{\partial t}$$

定态薛定谔方程：

$$-\frac{\hbar^2}{2\mu}\nabla^2\Psi+U\Psi=E\Psi$$

薛定谔方程仅适用于速度不太大的非相对论粒子，其中也没有包含关于粒子自旋的描述。当涉及相对论效应时，薛定谔方程由相对论量子力学方程所取代，其中自然包含粒子的自旋。

3.3.6 眼见为实：量子力学的实验证明

量子力学从根本上改变人类对物质结构及其相互作用的理解。除了广义相对论描写的引力以外，迄今所有基本相互作用均可以在量子力学的框架内描述(量子场论)。

量子力学并没有证明什么，它只是从另一个可能的角度描述了我们的宇宙——一种难以言喻的无限不可分时空观。跟唯物和唯心没什么关系，量子力学其本质依旧是唯物的。

量子力学可以算作是被验证的最严密的物理理论之一。至今为止，所有的实验数据均无法推翻量子力学。大多数物理学家认为，它“几乎”在所有情况下，正确地描写能量和物质的物理性质。虽然如此，量子力学中，依然存在着概念上的弱点和缺陷，除上述万有引力的量子理论缺乏外，至今为止对量子力学的解释存在争议。

在说这个实验前，我们来看曾经爱因斯坦和玻尔之间针锋相对的一次争论。

1.“爱因斯坦光盒”实验——玻尔与爱因斯坦的争论

1930 年秋天，第六届索尔威会议开幕了。这次会议的主题是“物质的磁性”。从物理学史和人类思想史的观点来看，关于量子力学基础问题的讨论显然在这次会议上形成了“喧宾夺主”之势。各国的科学家怀着激动的心情，期待着两位巨人之间新一轮论战。

这次，爱因斯坦经过三年的深思熟虑，秣马厉兵，显得胸有成竹，一开始便先发制人。他提出了著名的“光子箱”(又称为“爱因斯坦光盒”)思想实验。他提出用相对论的方法，来实现对单个电子同时进行时间和能量的准确测量。如果这个方法可行，那么，即可宣告

测不准关系破产，玻尔的工作和量子论的诠释将被推翻。

爱因斯坦沉着地在黑板上画了一个“光子箱”思想实验的草图，在一小盒子（光子箱）中装有一定数量的放射性物质，下面放一只钟作为计时控制器，它能在某一时刻将盒子右上方的小洞打开，放出一个粒子（光子或电子），这样光子或电子跑出来的时间就能从计时钟上准确获知。

少了一个粒子，小盒的质量差则可由小盒左方的计量尺和下面的砝码准确地反映出来，根据爱因斯坦质能公式 $E=mc^2$，质量的减少可以折合成能量的减少。因此，放出一个粒子准确的时间和能量都能准确测得。这与海森伯的不确定性原理完全相左，准确性和因果性再次获得了完整的表达。爱因斯坦最后还着重表示，这一次实验根本不涉及观测仪器的问题，没有什么外来光线的碰撞可以改变粒子的运动。一轮新的论战就这样开始了。

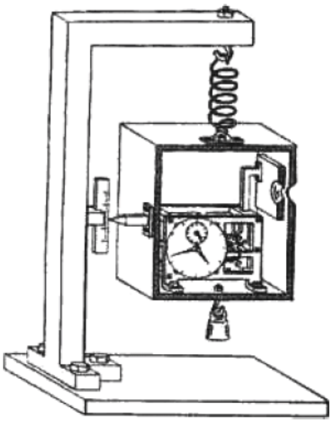


图 3-10　爱因斯坦光子箱

爱因斯坦光子箱的思想实验图如图 3-10 所示。

这一回，玻尔遇到了严重挑战。他刚一听到这个实验时，面色苍白，呆若木鸡，感到十分震惊，不能马上找出这个问题的答案。当时他着实慌了手脚，在会场上一边从一个人走向另一个人，一边喃喃地说：“如果爱因斯坦正确，那么物理学就完了。”据罗森菲尔德回忆，当这两个对手离开会场时，爱因斯坦那天显得格外庄严高大，而玻尔则紧靠在他的旁边快步走着，非常激动，并徒劳地试图说明爱因斯坦的实验装置是不可能的。

当天夜里，玻尔和他的同事们一夜没合眼。玻尔坚信爱因斯坦是错的，但关键是要找出爱因斯坦的破绽所在。他们检查了爱因斯坦实验的每一个细节，奋战了一个通宵，终于找出了反驳爱因斯坦的办法。

第二天上午，会议继续进行，玻尔喜气洋洋地走向黑板，也画了一幅“光子箱”思想实验的草图，与爱因斯坦不同的是，玻尔具体给出了称量小盒子质量的方法。他把小盒用弹簧吊起来，在小盒的一侧，他画了一根指针，指针可以沿固定在支架上的标尺上下移动。

这样，就可以方便地读出小盒在粒子跑出前后的质量了。然后，玻尔请大家回忆爱因斯坦创立的广义相对论。从广义相对论的等效原理可以推出，时钟在引力场中发生位移时，它的快慢要发生变化。因此，当粒子跑出盒子而导致盒子质量发生变化时，盒子将在重力场中移动一段距离，这样所读出的时间也会有所改变。这种时间的改变，又会导出测不准关系。可见，如果用这套装置来精确测定粒子的能量，就不能准确控制粒子跑出的时间。玻尔随之给出了运用广义相对论原理的数学证明。

这下，爱因斯坦不得不又一次承认，玻尔的论证和计算都是无可指责的。他自己居然在设计这个理想实验时，只考虑了狭义相对论而没有考虑广义相对论，出了一个大疏忽，实在太遗憾了。他意识到在量子力学的形式体系范围内是驳不倒测不准关系的，在口头上承认了哥本哈根观点的合理性。这时，与爱因斯坦和玻尔都是好朋友的埃伦菲斯特，以开玩笑的口气对爱因斯坦说，你不要再试图制造“永动机”了。爱因斯坦表示欣然接受。

玻尔的胜利赢得了越来越多物理学家对他观点的赞同。量子力学的哥本哈根解释已被绝大多数物理学家奉为正统解释。玻尔并没有满足在会议上所取得的胜利，他回去后又仔细研究了“爱因斯坦光盒”的每一个细节，并且让他的学生、物理学家伽莫夫制作了一个实体模型。至今这个模型仍保存在哥本哈根的玻尔理论物理研究所中。

2.量子擦除实验

量子擦除实验是杨氏双缝干涉实验的一个变形。人们已经认识到在双缝实验中，如果光子穿过了某条间隙而被观测到了，那么光子就无法与自身发生干涉。如果一束光子中的每一个光子都像这样被确定从某条间隙穿过，那么就无法看到杨氏实验中的干涉图案。

这个实验试图制造这样一种状况：如果我们确定光子穿过了哪条间隙并做上“标记”，那么将不会有干涉现象发生，但如果在这个光子到达屏幕前，将这个标记擦除，那么又将观测到杨氏实验中的干涉现象。量子擦除实验的意义在于，在双缝实验中探测或标记光子路径将会破坏干涉，但在此之后再擦除这个标记，人们可以重新恢复量子干涉。

量子擦除实验分三个阶段。

第一阶段，使用非线性 BBO 晶体产生纠缠光子对。自光子对产生起，它们就具有不同的偏振态，沿不同方向传播。沿下面的路径传播的光子会遇到双缝，使用灵敏的探测器可以扫出这些光子的干涉图样，如图 3-11 所示。

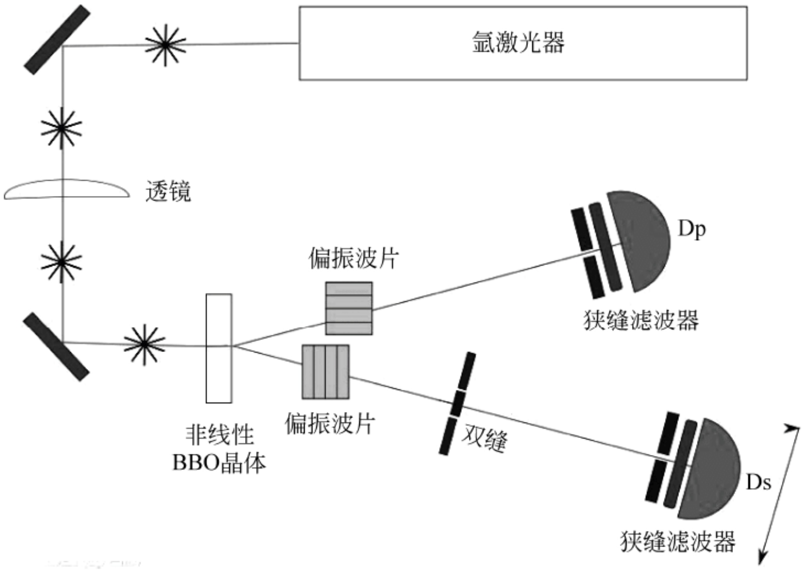


图 3-11　实验第一阶段

第二阶段，在下路径上插入四分之一波片。这样任何通过缝 A 的光子将会被改变为顺时针或逆时针的圆偏振，任何通过缝 B 的光子的则具有相反方向的圆偏振。当探测设备在先前的移动范围内重新扫过，可以发现探测结果不再相同——干涉条纹消失，即任何标记了光子路径的行为都会破坏干涉条纹，如图 3-12 所示。

第三阶段，下路径不变动，将一个起偏器插入到上路径，使得任何通过下路径的纠缠光子对的偏振方向也受到影响。因为上路径的光子的偏振方向发生变化，下路径光子的偏振状态也会改变。通过对上路径上起偏器选择合适的偏振角，令下路径上刚好有一半的光子具有相同的偏振方向。一旦它们有相同的偏振态，它们可以再次彼此干涉，或者从另一个角度来看，已经没有标记指明哪个通过缝 A，哪个通过缝 B，如图 3-13 所示。

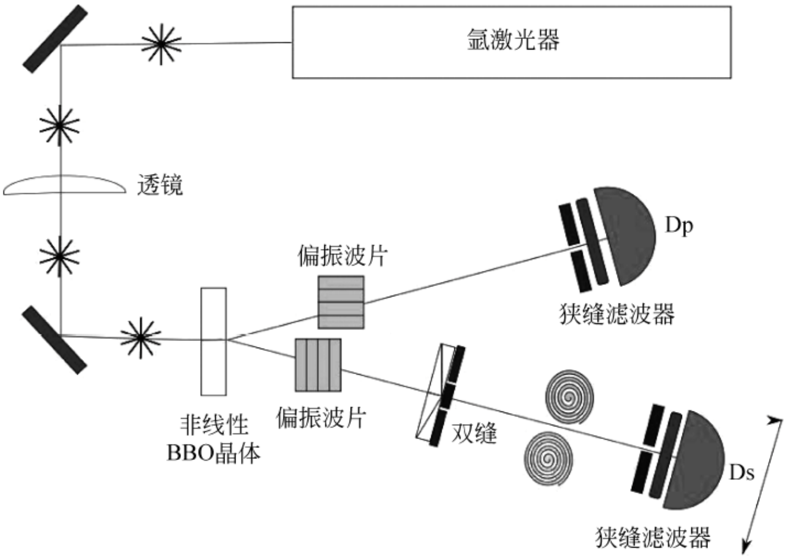

氩激光器
透镜
偏振波片
Dp
狭缝滤波器
非线性
BBO晶体
偏振波片
双缝
Ds
狭缝滤波器

图 3-12 实验第二阶段

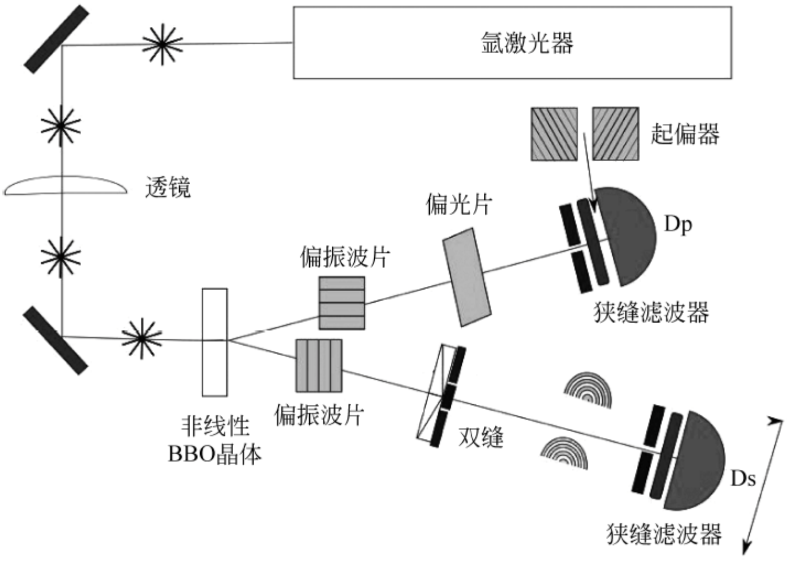

氩激光器
起偏器
透镜
偏光片
Dp
偏振波片
狭缝滤波器
非线性
BBO晶体
偏振波片
双缝
Ds
狭缝滤波器

图 3-13 实验第三阶段

3.3.7　牛顿力学与量子力学的决战

如何看待牛顿力学与量子力学的区别?

如果将科学看作地图,牛顿力学与量子力学就是不同精度和范围的地图。地图会随时间变化,有些变化很大,有些则变化很小,并且在不同情形下各有其用。

1. 量子力学与经典力学的主要区别

(1) 经典物理几乎是独立地处理粒子的运动以及粒子群或者场的波动,但量子力学必须统一处理粒子和波动。

(2) 经典物理认为粒子与波动是两个层次的东西,根本不是一回事儿。量子力学却认为两者是密不可分的一个整体,此即著名的“波粒二象性”,由此引发了一系列量子力学所特有的奇异结果:如测不准原理、观测量的不连续性(即量子)、统计诠释(即单粒子的行为在本质上也是不能完全确定的,这不同于经典统计力学)、量子态的非定域性(这与相对论有冲突,但实验又似乎肯定了这种非定域性——有某种意义上的超光速现象存在,至今尚无定论)等。

(3) 经典力学是对宏观物体和低速物体进行的力学研究,量子力学是对微观物体和高速物体的力学研究。宏观和微观的界限在原子层面,高速和低速的界限在近光速层面,最主要的区别是经典力学里物体的能量是连续的,量子力学中物体的能量是不连续的,呈跳跃型,这些连续的能量就称为量子。联系在于两者互为极限情况。

(4) 经典力学和量子力学不能在宏观、微观或者高速、低速方面来区分。

牛顿的力学体系、麦克斯韦的电磁学、爱因斯坦的相对论都属于经典力学范围。量子力学是由玻尔为首的一些科学家建立的另一种对立的力学体系。两者的区别在三个方面。

① 经典力学:连续性、确定性、因果性。

② 量子力学:不连续性、不确定性、不因果性。

不连续性:物质和能量都有最小的单位,是一份一份的。

不确定性:人们无法同时给定物质所有的参数,一个参数越详细,另一个参数就越不

准确。

不因果性：即使知道所有参数(虽然理论上不能)，所得到的也只是个概率的结果。

形象一点，经典物理认为这个世界是“和谐”的，宇宙是有物理定律严格确定的，如果知道一个时刻的参数，便可以推论出宇宙任何时刻的样子。存在客观的物质世界。

量子物理就不一样，它认为这个世界是“自由”的。宇宙充满了不确定性，你无法准确知道物质的所有参数。物质不能由物理定律来束缚。不存在绝对的客观世界。

2.相对论与量子理论的区别

相对论讲的是从宏观到微观。量子理论讲的是从微观到宏观。它们的区别是研究问题是从两端开始，最后目标接近对方。

1）经典物理学的局限性

到 19 世纪末，以麦克斯韦方程组为核心的经典电磁理论的正确性已被大量实验所证实，但麦克斯韦方程组在经典力学的伽利略变换下不具有协变性，而经典力学中的相对性原理则要求一切物理规律在伽利略变换下都具有协变性，而相对论和量子力学解决了这些问题。

2）狭义相对论

狭义相对论是主要由爱因斯坦创立的时空理论，是对牛顿时空观的改造。

爱因斯坦的第二种相对性理论产生于 1916 年。该理论认为引力是由空间-时间几何(也就是说，不但考虑空间中的点之间，而且考虑在空间和时间中的点之间距离的几何)的畸变引起的，因而引力场影响时间和距离的测量。

3）广义相对论

广义相对论是爱因斯坦的基于科学定律对所有的观察者(而不管他们如何运动)必须是相同的观念的理论。它将引力按照四维空间—时间的曲率来解释。

广义相对论是爱因斯坦于 1915 年以几何语言建立而成的引力理论，结合狭义相对论和牛顿的万有引力定律，将引力描述成因时空中的物质与能量而弯曲的时空，以取代传统对引力是一种力的看法。

因此，狭义相对论和万有引力定律，都只是广义相对论在特殊情况之下的特例。狭义

相对论是在没有重力时的情况；万有引力定律则是在距离近、引力小和速度慢时的情况。

4）适用范围

经典物理学在微观和高速下并不适用，相对论在解释宏观高速运动的现象时非常圆满，而量子力学在微观世界时更加得心应手。当然，相对论完全可以替代经典力学的应用领域，经典力学是相对论在低速环境下的近似表达方式，在解决一般问题时，经典力学还是很好用的。

在100多年以前，牛顿力学统治着宏观世界，也就是质量不等于0的世界。最近100年，人类认识到量子力学是微观世界的主宰，这是质量趋近于0的世界。这两种力学对应不一样的对象，有截然不同的规则，其背后又有截然不同的两套世界观，深刻影响着每个人的日常行为和思考。由于牛顿力学统治世界几千年，而量子力学在最近几十年才成熟，所以大部分人还是习惯用牛顿力学的原则思考问题。

牛顿力学的规则：世界是连续变化的，没有断点。由这条规则可以导出后三条规则：世界是渐进变化的；世界是简单的因果关系，原因和结果之间是一一对应的；世界是确定的、被决定好的，人只能发现它、反映它，但改变不了它。

相应地，量子力学的规则：世界不是连续变化的，是跳跃发展的，世界是复杂的因果关系，也就是原因和结果之间不能一一对应，最重要的是，世界不是确定的，是可以被改变的。

牛顿力学的力量不仅在物理界，它还影响人形成一套思考和做事方式，你甚至可以把它当成一套哲学和宗教。未来是可以被预测的，因为牛顿的世界是连续的，因果之间一一对应，给出一个起点就可以算出一个终点。就好像火箭从升空到回落，它有一个确定的轨迹，始终在掌握之中。所以每个人、每个公司都在计划，都在筹谋。正因为世界是连续的，所以我们习惯慢慢来，不要太快，循序渐进，一分耕耘一分收获。遇到问题就找原因，一旦找到原因结果就会变化。

但量子力学无疑是截然不同的另一套哲学和做事方式。未来是难以被预测的，你无法从过去推导出未来。倘若你能找到一个看似很不符合逻辑的原因，那才可能是真正的原因。人的观点可以突变，一秒钟过去，坏人就变成了好人。不是越能吃苦就越有前途。

只要你找对了频率，一刹那就可以接通，就能获得爆发，跟时间无关。你不会觉得累，只要你配合上一个节奏，你会觉得很高兴。很像大家所看到的冲浪，只要跟上浪的节奏。

牛顿力学适用的是过去几千年的农业和工业社会，这是“强物质”的时代，质量不等于0。但量子力学适用于当前的信息社会，这是“弱物质”的时代，质量趋近于0，尤其是互联网世界，所有的现象、资产和被引发的情感都是由0和1两个数字组合而成。

3.量子力学中最不好懂的东西

先把量子力学中人们最不好懂的东西简单形象地介绍给大家，打好基础。

1）态叠加与坍缩

量子力学的第一个诡异现象称为态叠加和坍缩。

为了解释量子力学的观念，先说说普通人的日常经验。一般人认为客观物体一定要有一个确定的空间位置，这种存在，是不以人的意志为转移的，是客观的。例如，我的女儿现在在客厅里面，或者说我的女儿现在不在客厅里面，两者必居其一。

女儿可以既在客厅里面又不在客厅里面吗？

这在量子力学里就不一样了。量子力学就像说你的女儿既在客厅又不在客厅（你不知道你的女儿在不在客厅），你要去看女儿在不在客厅，你就实施了到客厅观察的动作。你一观察，女儿的存在状态就坍缩了，她就从原来的、在客厅又不在客厅的叠加状态，一下子变成在客厅或者不在客厅的唯一状态了。

所以，量子力学怪就怪在这儿：你不观察它，它就处于叠加态，也就是一个电子既在A点又不在A点；你一观察，它这种叠加状态就崩溃了，它就真的只在A点或者真的只在B点，只出现一个。

那有人就会说了：你这是诡辩，你怎么知道电子不观察它的时候，它既在A点又不在A点呢？这就是量子力学发展过程中，很多实验确证的事情。

2）单体的叠加态：薛定谔的猫

这个实验是量子力学的创始人薛定谔提出的，被称为“薛定谔的猫”（既死又活的叠加态猫）。

把一只猫放进一个封闭的盒子里，然后把这个盒子接到一个装置上，这个装置包含一

个原子核和一个毒气设施。原子核有50%的可能性发生衰变，衰变的时候就会发射出一个粒子，这个粒子一发出来就会触发毒气设施，毒气一触发就会杀死这只猫，就是说猫也处于这种既死又活的叠加状态。这是他想象中的一个实验。

这个问题一提出来，物理学家一个个都惊呆了，原来以为只有微观世界才有这种态叠加，就是状态不确定，既处于这个状态，又不处于这个状态。现在宏观世界也一样了，猫不就是这样吗？有一只既死又活的猫。

这与我们的经验严重违背。这个实验实际上就是“女儿在客厅里，女儿不在客厅里”变了个样子说出来。这个猫是死了还是活着？既死又活是同时存在的，量子力学就认为两者同时存在。

怎么可能既死又活同时存在呢？人不能想象这种状态，于是大家就把这个实验进一步讨论下去。

从不确定到确定可避免意识参与吗？

1963年，获得诺贝尔物理学奖的维格纳想了一个新的办法，他说：我让一个朋友戴着防毒面具也和猫一起待在那个盒子里面去，我躲在门外，对我来说，这猫是死是活我不知道，猫是既死又活。事后我问在毒气室里戴防毒面具的朋友，猫是死是活？朋友肯定会回答，猫要么是死要么是活，不会说是半死不活。

这个说法一出来大家就发现，问题在哪儿呢？一个人和猫一起待在盒子里，人有意识，意识一旦包含到量子力学的系统中去，它的波函数就坍缩了，猫就变成要么是死，要么是活了。也就是说，猫是死是活，只要一有人的意识参与，就变成要么是死，要么是活，就不再是模糊状态。

3）多体的叠加态：量子纠缠

下面再来讲量子纠缠。

“薛定谔的猫”讲的是同一个东西处于不同状态的叠加，量子纠缠讲的是如果有两个以上的东西它们都处于不同状态的叠加，它们彼此之间一定有明确的关系。这就是量子纠缠。

讲个例子：纠缠态的手套。

例如，我们从北京买了一双手套，把手套中的一只寄到香港地区，另一只寄到华盛顿，那么寄到香港的是左手戴的还是右手戴的？

谁都不知道，如果香港地区的人收到了打开一看，是左手的，那华盛顿的人不用看就知道收到的是右手的，因为手套是左右配对的，这是个规则。一旦寄出去了，寄的过程中不确定，但是一个人只要观测了他收到的手套是左手的还是右手的，另一个人不用观测就知道了。这就是纠缠的一个例子。

大家会认为，你看没看它没关系，它早就确定了。但量子力学大量实验证明，如果把同一个量子体系分开成几个部分，在未检测之前，你永远不知道这些部分的准确状态；如果你检测出其中之一的状态，在这瞬间其他部分立即调整自己的状态与之相应。

这样的量子体系的状态称为“纠缠态”。就好比是这个手套在寄出以后，在还没被观测之前，它是不是确定呢？肯定不确定。只有在你确定了其中某一个的状态，另一个的状态立刻就变化了，也变得确定起来了。

大家也许很难理解这个纠缠，说实话，这个已经超出了人类的理解能力的范围之外，你只能去试图想它、接受它，跟我们日常生活中的客观经验已经不符了。

4. 意识是量子物理现象

意识是一种量子力学现象。为什么这么说呢？例如，你面前出现了一朵花，这时有两种可能的状态。

一种状态：一个没有任何心思的人，“对境无心”，看花不是花，此时他的意识处于自由状态，他没看到花是不是红的，好不好看，他看它并不是花，他根本就不动念头。这种境界在唐代张拙的诗中写道“一念不生全体现，六根才动被云遮”。

另外一种状态：如果你看到这朵花，一下子动念头了，有了相应的意识，动念头实质上就是进行测量。你用鼻子进行测量发现是香的，你眼睛进行测量发现是红色的而且美丽，你动意念去测量它，发现它很令人愉快。

于是这些测量的结果，也就是念头的结果，一下子使你产生了进一步的念头：这是一朵玫瑰花，就认出它来了。

再来说说未经测试的电子和未生念头的意识之间的关系。

这个自由状态与刚才所说量子力学的诡异现象怎么可以比较起来呢？就是电子这些东西，在你没有测量的时候，它处处都存在，也处处不存在，一旦你测量，电子就有个固定状态出来了。

意识也是这样，如果你看到这朵花，一下子动念头了，动念头实质上就是做了测量。

你用鼻子做了测量发现是香的，你用眼睛进行测量发现是红色的并且美丽，你动意念去测量它，发现它令人愉快。

于是这些测量的结果，也就是念头的结果，一下子使你产生了进一步的念头：这是一朵玫瑰花，就认出它来了。

人的意识发动的过程实际上是通过动念进行测量，然后产生念头。这时候念头就产生出来了，实质是通过测量得出的几个人们制造出来的概念。这时意识不再自由，它突然坍缩到一个概念“玫瑰花”上。

因此，是念头产生了“客观”，念头就是测量，客观世界是一系列复杂念头造成的。

3.4 独门绝活：量子纠缠

量子纠缠也称为量子缠结，是一种量子力学现象，是1935年由爱因斯坦、波多尔斯基和罗森提出的一种波。

量子纠缠技术是安全的传输信息的加密技术，与超光速传递信息相关。尽管知道这些粒子之间“交流”的速度很快，但我们目前却无法利用这种联系以如此快的速度控制和传递信息。因此，爱因斯坦提出的规则，即任何信息传递的速度都无法超过光速，仍然成立。实际上的纠缠作用并不很远，而且一旦干涉其中的一方，纠缠态就会自动消除。

科学家希望能够建造量子计算机，利用粒子纠缠进行超高速计算。

3.4.1 给量子纠缠做个CT

1. 量子纠缠简介

1）量子纠缠的定义

量子纠缠是粒子在由两个或两个以上粒子组成的系统中相互影响的现象，虽然粒子

在空间上可能分开。

纠缠是关于量子力学理论最著名的预测。它描述了两个粒子互相纠缠，即使相距很远，一个粒子的行为将会影响另一个粒子的状态。当其中一个粒子被操作（例如量子测量）而状态发生变化，另一个粒子也会即刻发生相应的状态变化，如图 3-14 所示。

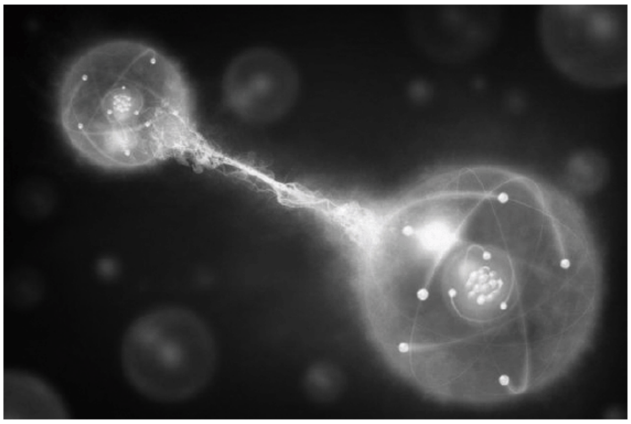


图 3-14　量子纠缠

爱因斯坦将量子纠缠称为“鬼魅似的远距作用（神鬼级的远距离相互操作作用）”。但这并不仅仅是个诡异的预测，而是已经在实验中获得的现象，例如，科学家通过向两个处于室温的纠缠的小钻石发射激光。

量子纠缠说明在两个或两个以上的稳定粒子间，会有强的量子关联。例如，在双光子纠缠态中，向左（或向右）运动的光子既非左旋，也非右旋，既无所谓的 x 偏振，也无所谓的 y 偏振，实际上无论自旋或其投影，在测量之前并不存在。在未测时，二粒子态本来是不可分割的。

2）量子纠缠现象解释

量子纠缠所代表的在量子世界中的普遍量子关联则成为组成世界的基本的关联关系。或许可用纠缠的观点来解释“夸克禁闭”之谜。

当一个质子处于基态附近的状态时，它的各种性质可以相当满意地用三个价夸克的结构来说明。质子和中子都是由 u 夸克和 d 夸克组成，u 夸克带电量为 2e/3，d 夸克带电量为－e/3，e 为基元电荷。但是实验上至今不能分离出电荷为 2e/3 的 u 夸克或－e/3 的

d 夸克，这是由于夸克之间存在着极强的量子关联，后者是如此之强，以至于夸克不能再作为普通意义下的结构性粒子。

通常所说的结构粒子 a 和 b 组成一个复合粒子 c 时的结合能远小于 a 和 b 的静能之和，a 或 b 的自由态与束缚态的差别不大。而核子内的夸克在“取出”的过程中大变而特变，人们看到的只能是整数电荷的介子等强子。

同一个质子，在不同的过程中有不同的表现，在理解它时需要考虑不同的组分和不同的动力学。一个质子在本质上是一个无限的客体。实质上，整个宇宙是一个整体的能量惯性体系包括实在的粒子和空间，由于能量惯性的存在，整个能量体系时刻按一定的能量运动规律运动，宇宙中的每一个粒子作为宇宙能量的一分子，它本身的能量惯性状态始终与宇宙环境保持一致，即能量的稳定性，它们的电磁能量波始终存在相互作用。

当两种物质粒子同时处于某一状态，即尽量使之处于基态或能量控制编码态，它们在相互作用时产生了电磁能量惯性互动及量子纠缠现象。

3）量子纠缠公式表达

1935 年，爱因斯坦、波多尔斯基和罗森等人提出一种波，基本特征是在任何表象下，它都不可以写成两个子系统的量子态的直积形式。这样的量子态称为纠缠态。

4）量子纠缠度描述

纠缠度是指所研究的纠缠态携带纠缠的量的多少。对纠缠度的描述，实质上是对不同纠缠态之间建立定量的可比关系。纠缠状态所纠缠的粒子数量越多，对经典物理学的偏离越明显，获得有用量子效应的机会就越大。所以，在量子信息领域中，纠缠通常被看作是非局域的“信息源”。

于是，如何对纠缠定量化就显得十分重要。对于两体纯态而言，它仍是两体纯态唯一合理的纠缠度定义。对于多体纠缠度描述的研究，到目前为止仍没有得到真正解决，人们仍未放弃寻找一种物理意义上更为鲜明、简单、易于求解的纠缠度的描述。

5）量子纠缠的特点

量子力学是非定域的理论，这一点已被违背贝尔不等式的实验结果所证实。因此，量子力学展现出许多反直观的效应。量子力学中不能表示成直积形式的态称为纠缠态。纠

缠态之间的关联不能被经典地解释。量子纠缠指的是两个或多个量子系统之间存在非定域、非经典的强关联。量子纠缠涉及实在性、定域性、隐变量以及测量理论等量子力学的基本问题，并在量子计算和量子通信的研究中起着重要的作用。

多体系的量子态的最普遍形式是纠缠态，而能表示成直积形式的非纠缠态只是一种很特殊的量子态。历史上，纠缠态的概念最早出现在1935年薛定谔关于“猫态”的论文中。纠缠态对于了解量子力学的基本概念具有重要意义，已在一些前沿领域中得到应用，特别是在量子信息方面(例如，量子远程通信)。我国科学家已经成功地制备了8粒子最大纠缠态。

2.量子纠缠理论的发展

1）量子纠缠理论的产生

从19世纪末到20世纪初，量子力学快速发展并完善起来，解决了许多经典理论不能解释的现象，大量的实验事实及实际应用也证明了量子力学是一个成功的物理理论。但是关于量子力学的基本原理的理解却存在不同的解释。

众多的物理学家在自己观点的指引下，对量子力学的基本解释提出自己的看法，主要有三种：传统解释、PTV系统解释和统计解释，这三种解释之间既有区别又有联系。

传统解释的出发点是量子假设，强调微观领域内每个原子过程或基元中存在着本质的不连续，其核心思想是玻尔(丹麦物理学家，量子力学奠基人之一)的互补原理(并协原理)，还接受了玻恩(德国犹太裔理论物理学家)对态函数的概率解释，并把这种概率理解为是同一个粒子在给定时刻出现在某处的概率密度。

PTV系统解释的代表是玻姆(美国犹太裔理论物理学家)，这种解释试图通过构造各种隐变量量子论来寻找量子力学的决定论基础，即为态函数的概率解释构建决定论的基石，目的是在微观物理学领域内恢复决定论和严格因果性，消除经典世界同量子世界的独特划分，回到经典物理学的预设概念，建立物理世界的统一说明。

统计解释认为态函数是对统计系统的描述，量子理论是关于系统的统计理论，这个系统是由全同的(或相似的)制备系统组成，不需要一个预先确定的动力学变量的集合，是一种最低限度的系统解释。

上面讲到三种观点既有联系又有区别，正是由于各方都坚持己见，才有了著名的爱因斯坦与玻尔之间的论战。爱因斯坦说：“上帝不掷骰子。”玻尔说：“亲爱的爱因斯坦不要指挥上帝做什么。”量子纠缠才被爱因斯坦以一个悖论的疑问提出。

1927年9月，玻尔在科摩会议中首度公开地演讲他的互补原理，由于他采用了大量的哲学语言来阐释互补原理，使大家感到震惊和困惑。当时大多数人对于测不准关系和互补原理的深刻内涵还不大明白。几个星期后，在布鲁塞尔举行的第五届索尔维亚会议，玻尔、爱因斯坦、玻恩、薛定谔、海森伯等世界最著名的科学家都出席了这项盛会。玻尔在会议中重述了他在科摩会议上的观点。在这次会议上，爱因斯坦首次听到玻尔亲自阐述互补原理和对量子力学的诠释，了解到量子纠缠在黑洞，及更小的等级时绝对会干扰量子纠缠。

2）量子纠缠理论完善

1951年，玻姆在《量子理论》中重新表述了EPR思想，用两个自旋分量代替原来的坐标和动量，为进一步研究特别是实验检验奠定了基础。

1952年，玻姆在《物理学评论》上连续发表两篇文章，提出量子力学的隐变量解释。玻姆认为，在量子世界中粒子仍然是沿着一条精确的连续轨迹运动的，只是这条轨迹不仅由通常的力来决定，而且还受到一种更微妙的量子势的影响。

量子势由波函数产生，它通过提供关于整个环境的能动信息来引导粒子运动，正是它的存在导致了微观粒子不同于宏观物体的奇异的运动表现。此外，玻尔理论所假设的另外一个物理实际存在的实在性波函数同样是不可探测的隐变量，但据报道，近期哈尔滨理工大学朱智涵课题组及其合作者等提出了量子螺旋双缝理论及实验方案，并首次通过实验证实了波函数的物理实在性。

3）量子纠缠态制备

多光子纠缠态的制备和操控一直是量子信息领域的研究重点。世界上普遍利用晶体中的非线性过程来产生多光子纠缠态，其难度会随着光子数目的增加而指数级增大。

2000年，美国国家标准局在离子阱系统上实现了四离子的纠缠态。

2004年，合肥微尺度物质科学国家实验室量子物理与量子信息研究部的研究人员打

破了这一纪录，在国际上首次成功实现五光子纠缠的操纵。

2005 年年底，美国国家标准局和奥地利因斯布鲁克小组分别宣布实现了六个和八个离子的纠缠态，并且一直保持着这个纪录。

2011 年 11 月 22 日，中科院量子信息重点实验室成功制备出八光子纠缠态——GHZ 态，并进一步利用产生出的纠缠态完成了八端口量子通信复杂性实验。研究报告在线发表在《自然·通信》上，实验结果超越了以往界限，展示了量子通信抗干扰能力强、传播速度快的优越性。

4）量子纠缠隐形传输证明史

量子态隐形传输是对古典物理中“定域性定律”的又一打击。该定律指出，一个物体只能被它周围的环境直接影响。量子论承认“幽灵般的远程效应”。

物理学家贝尔 1964 年首先设计了一个实验作为证明“‘幽灵般的远程效应’真实存在”的一种方法，因此，研究人员把该实验称为“没有漏洞的贝尔测试”。

（1）1997 年奥地利蔡林格小组首次验证量子纠缠。

1997 年，奥地利蔡林格小组在室内首次完成了量子态隐形传输的原理性实验验证。

（2）2004 年奥地利蔡林格小组测试数百米级量子纠缠。

2004 年，奥地利蔡林格小组利用多瑙河底的光纤信道，成功地将量子“超时空穿越”距离提高到 600m。由于光纤信道中的损耗和环境的干扰，量子态隐形传输的距离难以大幅度提高。

（3）2005 年中国科学技术大学测试十千米级量子纠缠。

中国科学技术大学潘建伟、彭承志等研究人员的小组早在 2005 年就在合肥创造了 13km 的自由空间双向量子纠缠“拆分”、发送的世界纪录，同时验证了在外层空间与地球之间分发纠缠量子的可行性。

3.4.2 千里之外的心灵感应：隐形传输

“量子隐形传态”实验：能实现科幻中的超时空传输吗？

科幻电影《星际迷航》讲述了人类这样一个梦想：宇航员在特殊装置中平静地说一句

“发送我吧，苏格兰人”，他就瞬间被转移到另一个星球。

中国发射了世界首颗量子卫星，科学家将在“世界屋脊”西藏阿里和这颗卫星之间开展“量子隐形传态”实验。这与《星际迷航》中的超时空传输很类似。当然，它们并不相同——中国科学家开展的量子隐形传态实验中，被传输的是信息而非实物。

1. 什么是量子隐形传态

科学家都喜欢用孙悟空的“筋斗云”来比喻量子隐形传态。在四大名著之一的《西游记》里，孙悟空一个“筋斗云”就能越过十万八千里。明朝的作家吴承恩怎么也不会想到，几百年后科学家已经在微观粒子层面的实验上验证了“筋斗云”这种超能力的可实现性。利用量子纠缠发展出的量子隐形传态，可以将物质的未知量子态精确传送到遥远地点，就像孙悟空的“筋斗云”一样，可以实现从A地到B地的瞬间传输。

专家解释说，把粒子A的未知量子态传输给远处的另一个粒子B，让B粒子的状态变成A粒子最初的状态。注意传的是状态而不是粒子，A、B的空间位置都没有变化，并不是把A粒子传到远处。当B获得这个状态时，A的状态必然改变，任何时刻都只能有一个粒子处于目标状态，所以并不能复制状态，或者说这是一种破坏性的复制。

量子隐形传态的设想和概念是1993年由六位物理学家联合提出的。1997年奥地利物理学家蔡林格带领的团队首次实现了传送一个光子的自旋。他们在《自然》上发表了一篇题为《实验量子隐形传态》的文章。这篇文章后来入选了《自然》杂志的“百年物理学21篇经典论文”，跟它并列的论文包括伦琴发现X射线、爱因斯坦建立相对论、沃森和克里克发现DNA双螺旋结构等。

事实上，在量子态隐形传态理论发展的漫长过程中，每一点进步都可以被视为一座里程碑。虽然最初的传输距离仅为数米，但美国《科学》杂志的评语是：“尽管想要看到《星际迷航》中‘发送我吧’这样的场景，我们还得等上很多年，但量子隐形传态这项发现，预示着我们将进入由具有不可思议能力的量子计算机发展而带来的新时代。”

但接下来，发展并不算顺利。直到2004年，蔡林格小组才利用多瑙河底的光纤信道，将量子隐形传态距离提高到600m。

2007年开始，中国科大—清华大学联合研究小组在北京架设了长达16km的自由空

间量子信道，并取得一系列关键技术突破，最终在 2009 年成功实现了世界上最远距离的量子态隐形传输，证实了量子态隐形传输穿越大气层的可行性，为未来基于卫星中继的全球化量子通信网奠定了可靠基础。该成果已经发表在 2010 年 6 月 1 日出版的英国《自然》杂志子刊《自然 · 光子学》上，并引起人们广泛关注。

2015 年 10 月，荷兰代尔夫特理工大学的科学家们把两颗钻石分别放在代尔夫特理工大学校园内的两侧，距离 1.3km。每块钻石含有一个可以俘获单个电子的微小空间，此空间具有一种称为“自旋”的磁性，然后用微波和激光能的脉冲来纠缠，并测量电子的“自旋”。校园的两侧设有探测器，两个电子之间的距离确保做测量的同时，信息无法以传统的方式交换。

2015 年，中国科学技术大学团队首次实现单光子多自由度的量子隐形传态，首次证明了一个粒子的所有性质在原理上都是可以被传输的。完整意义的量子隐形传态，应该说是 2015 年才实现的。

2016 年 12 月，中国科学技术大学研究团队在量子信息科研领域再获重大突破，他们通过两种不同的方法制备了综合性能最优的纠缠光子源，首次成功实现“十光子纠缠”，再次刷新了光子纠缠态制备的世界纪录。

2017 年 6 月 15 日，《科学》杂志以封面论文形式，报道了中国“墨子号”量子卫星首次实现上千千米量子纠缠的消息，相较于此前 144km 的最高量子传输距离纪录，这次跨越意味着绝对安全的量子通信离实用又近了一步。率先成功实现“千千米级”的星地双向量子纠缠分发，打破了此前国际上保持多年的“百千米级”。

2. 实物的瞬时传送还是科幻

量子隐形传态的突破可以看成是量子隐形传态从一到多的里程碑，预示着以后可能把更复杂的多体系统的信息一次给传输走。换句话说，《星际迷航》中人体“瞬时传输”技术在遥远的未来，或许可以实现。

大家都想离开太阳系去看看，但毕竟寿命是有限的，如果我们乘坐目前的宇宙飞船的话，人类还没飞出去，生命就结束了。我们将来如果以这种量子隐形传态的方法星际旅行，是可以光速进行的。不过，要传送更为复杂的东西现在还是一种科学幻想，近期肯定

不可能实现。

目前科学家的研究距离宏观物体的远距传输还差得很远，而目前量子隐形传态研究的主要应用是量子通信和量子计算。

3.4.3　量子纠缠将远程控制你的生活

1. 量子纠缠应用领域

纠缠态作为一种物理资源，在量子信息的各方面（如量子隐形传态、量子密钥分配、量子计算等）都起着重要作用。然而，受实验条件限制和不可避免的环境噪声的影响，制备出来的纠缠态并非都是最大纠缠态。

另一方面，纯纠缠态受环境的消相干作用也会退化成为混合态。使用这种混合纠缠态进行量子通信和量子计算将会导致信息失真。

为了达到更好的量子通信或量子计算效果，需要通过纠缠纯化技术将混合纠缠态纯化成纯纠缠态或者接近纯纠缠态。因此，如何提纯高品质的量子纠缠态是量子信息研究中的重要课题。常见的量子纠缠态应用有量子态隐形传输应用于量子通信和量子计算应用于量子计算机，量子计算在实现技术上有严重的挑战，实现这一问题要解决另外三个问题——量子算法、量子编码、实现量子计算的物理体系，量子保密通信也广泛应用于量子密码术中。

将来，由链状纠缠粒子环绕整个地球而形成量子通信网络。这种网络能够安全地共享加密密码，并且绝对能够监测到窃听的企图。

2. 量子纠缠无法超光速传递信息

只有能够传递信息，“超光速”才有意义。量子纠缠技术是安全的传输信息的加密技术，与超光速无关。尽管知道这些粒子之间“交流”的速度是光速的几千倍，但我们却无法利用这种联系以如此快的速度控制和传递信息。因此，爱因斯坦提出的规则（即任何信息传递的速度都无法超过光速）仍然成立。干涉量子纠缠的时候，量子纠缠态会立即消除，所以无法利用这种能力发送信号。

3.5 川剧变脸：量子态套叠

3.5.1 一般人都搞不清楚的量子态套叠

什么是量子态叠加原理?

电子做稳恒的运动,具有完全确定的能量。这种稳恒的运动状态称为量子态。量子态是由一组量子数表征,这组量子数的数目等于粒子的自由度数。

量子叠加只能存在于波函数的表达式中。也就是说,量子叠加是波函数的一种属性。例如,我们上抛一枚硬币,那么出现正反面的概率是完全相同的,用概率的语言说就是,它们出现的概率是各占50%。运用量子力学思考,由于波函数的归一属性,量子力学认为“出现”任何一面的概率都是100%,而没出现就是没有出现。这就是说“两个面”是同时出现的。量子力学称这种状态为“叠加态”。

这个概念在硬币没有落地前(事件发生前)是完全可以理解的,是正确的,但是事件一旦发生(硬币已经落地)。事实上究竟是哪面向上,就已经一定(量子语言称为波函数“坍缩”),当我们没有看到这个结果的时候,相对于我们它还是遵守波函数的表达的,就是对于没有看到结果的人硬币还与没落地之前是一样的“叠加”状态。但是,一旦看到了,波函数就坍缩了。所以,叠加态是不能观察的。

波函数坍缩指的是某些量子力学体系与外界发生某些作用后波函数发生突变,变为其中一个本征态或有限个具有相同本征值的本征态的线性组合的现象。

波函数坍缩可以用来解释为何在单次测量中被测定的物理量的值是确定的(虽然多次测量中每次测量值可能都不同)。

由于量子力学将“波函数坍缩”与人们是在什么时刻进行观察紧密相关,因此,就诞生了“薛定谔的猫”,为了解释薛定谔的猫,又创立了平行宇宙的概念。

事实上,波函数是在事件发生后就已经坍缩了。量子力学将两个不同的坍缩概念混淆在一起,就产生了很多不可思议的结果。

3.5.2 原来如此：量子态套叠原理

据报道，量子态叠加效应尺度已刷新纪录，美国斯坦福大学的研究团队成功地让原子云处在相距半米的两个状态进行了叠加，这将量子态叠加效应的最大尺度纪录从1cm扩展到了54cm。

研究团队认为，新研究成果可能意味着找到了量子世界与经典世界之间的分界点，因为相对那些量子水平的物体，新研究成果更适用于大尺度的宏观物体。《自然》杂志也发表了针对该团队研究的社论，描述他们的实验过程，并总结相关结果。

在过去几年里，有关量子粒子甚至与整个原子纠缠的新闻被大量报道。目前研究人员想让在更远距离外的两个粒子纠缠，这就有了关于纠缠对象大小的问题。

薛定谔的猫有过这样的讨论：作为理论家和那些在应用领域的专家试图找出是否真的可能导致整个猫同时出现在两个地方的情况。

据物理学家组织网报道，研究人员通过创建一个玻色-爱因斯坦凝聚态云(BEC)，由所有最初在相同状态的10000个铷原子(在一个超级冷冻室)组成。BEC是科学巨匠爱因斯坦在80年前预言的一种新物态，表示原来不同状态的原子突然“凝聚”到同一状态。然后，用激光把原子云推到10m高的腔室，使原子进入一个给定状态。当云到达腔顶时，波函数是给定状态的对半混合物，代表位置是54cm。当电子云被允许回到腔底时，研究证实原子从两个不同的高度下降，证明电子云处在叠加状态中。

该研究小组认识到，虽然实验刷新了宏观尺度叠加态的新纪录，但其仍然是用单个原子进行的。

3.6 挑战量子力学的带头大哥——爱因斯坦

3.6.1 量子力学描述世界的语言跟经典力学有根本区别

量子力学描述世界的语言跟经典力学有根本区别。经典力学描述一个粒子的状态，说的是它在什么位置，具有什么动量。不言而喻，在任何时刻这个粒子总是位于某个位

置，具有某个动量，即使你不知道是多少。

量子力学描述一个粒子的状态时，给出一个态函数或者态矢量，这个态矢量不是位于日常所见的三维空间，而是位于一个数学抽象的线性空间。

现在不可思议的新概念来了，对于任何一个物理量 P（例如位置、动量），态矢量都可以分为两类：一类具有确定的 P，称为 P 的本征态，P 的取值称为这个本征态的本征值；另一类不具有确定的 P，称为 P 的非本征态。

非本征态比本征态多得多，如同无理数比有理数多得多。也就是说，绝大多数情况下，一个粒子没有确定的位置！

什么是“没有确定的位置”？是因为粒子跑得太快了，我们看不清吗？量子力学说的不是这种常规（而错误）的理解，而是说：非本征态是一个客观真实的状态，跟本征态同样客观真实，它没有确定的位置是因为它本质上就是如此，而不是因为我们的信息不全。

打个比方，有些状态可以用指向上、下、左、右的箭头来表示，于是你定义“方向”为一个物理量，但是还有些状态是一个圆！圆的状态跟箭头的状态同样真实，只是没有确定的方向而已。

但是读者还会困惑，因为我们总是可以用仪器去测量粒子的位置，测量的结果总是粒子出现在某个地方，而不是同时出现在两个地方，或者哪里都测量不到。

下面就是量子力学的关键思想：对 P 的本征态测量 P，粒子的状态不变，测得的是这个本征态的本征值；而对 P 的非本征态 s 测量 P，会使粒子的状态突然从 s 变成某个 P 的本征态 f，概率是 s 与 f 的内积的绝对值的平方 $|(s, f)|$^2，发生这个突变后测得的就是 f 的本征值。

状态从 s 突变到 f 的概率是 $|(s, f)|$^2，实际意思就是这两个态越相似，概率就越大。用上面的例子来说，对箭头状态测方向，状态不变，得到的就是箭头的方向；对圆状态测方向，圆状态会以相同的几率变成任何一个箭头状态，得到的是这个新的箭头状态的方向。对位置的非本征态测量位置，就会测得粒子出现在某个随机的位置，而出现在空间所有位置的几率之和等于 1。

怎么知道测量结果是随机的呢？制备多个具有相同状态的粒子，把实验重复多次，就

会发现实验结果每次都不一样。没错，量子力学具有本质的随机性，同样的原因可以导致不同的结果，这是跟经典力学的又一大区别。

有人要问了，测量如此奇特，它的本质是什么？量子力学最大的神秘之一，就是测量的本质谁也不知道！目前只能把测量理解为一种操作定义：对本征态的测量不改变状态，得到本征值；对非本征态的测量随机地把它改变成某个本征态，得到相应的本征值。

你也许会觉得上面这些说法莫名其妙，但是现在绝大多数科学家都对它们很认同。为什么呢？因为这套奇怪的理论跟实验符合得很好，而经典力学却不能。

当然，这是哲学性的原因，而操作性的原因很简单：现在的科学家受的都是量子力学的教育。普朗克有一句非常有趣的话：“新的科学真理并不是由于说服它的对手取得胜利的，而是由于它的对手死光了，新的一代熟悉它的人成长起来了。”

3.6.2　EPR实验

事实上，现在仍然有不少人对量子力学提出各种各样的挑战，包括不少专业科学家，民间科学家就更多了（当然挑战相对论的民间科学家更多）。历史上，挑战量子力学的势力更加强大，其中的带头大哥就是——爱因斯坦！爱因斯坦坚信粒子应该具有确定的位置和动量，世界的演化应该是决定性的，对前面说的量子力学的不确定性和随机性十分不满。用他自己的话来说，他相信“没有人看月亮的时候，月亮仍然存在”，以及“上帝不掷骰子”，如图 3-15 所示。

图 3-15　爱因斯坦认为“上帝不掷骰子”

如果是一般人，表达完信念也就没事了，但爱因斯坦是伟大的科学家，神一样的人物，他不满足于只做口舌之争，打算按照科学规范，设计一个判决性的实验，以可验证的方式证明量子力学的错误。

于是在1935年，爱因斯坦、波多尔斯基和罗森提出了一个思想实验，后人用他们的首字母称为EPR实验。你可以制备两个粒子A和B的“圆”态，使得在这个状态中两个粒子的某个性质（如电子的自旋角动量、光子的偏振）相加等于零，而单个粒子的这个性质不确定。这样一对粒子称为“EPR对”，属于量子力学中的“纠缠态”，因为这两个粒子的性质不可分割地纠缠在一起了。

然后把这两个粒子在空间上分开很远，任意远，再测量粒子A的这个性质。好比你测得A是“上”，那么你就立刻知道B现在是“下”。好比成龙电影《双龙会》中有心灵感应的双胞胎，一个做了某个动作，另一个无论有多远都会做同样的动作（在相反的方向），如图3-16所示。问题是，既然A和B已经离得非常远了，B是怎么知道A发生了变化，然后发生相应的变化的？

图3- 16 《双龙会》

EPR认为A和B之间出现了“幽灵般的超距作用”，信息传递的速度超过光速，违反相对论。所以，量子力学肯定有错误。

这个问题非常深奥，直到现在都不断给人以启发。不过量子力学的正统卫道士有一个标准回答：处于纠缠态的A和B是一个整体，当你对A进行测量的时候，A和B是同时发生变化的，并不是A变了之后传一个信息给B，B再变化，所以这里没有信息的传递，不违反相对论。这个回答怎么样？无论你信不信，反正我信了。不过爱因斯坦一直都不信，以他参与创建的理论的反对者的身份走完了一生。

在爱因斯坦所处的时代，EPR 实验只能在头脑中进行。随着科技的进步，这个实验可以实现了。20 世纪 80 年代，阿斯佩克特等人做了 EPR 实验，结果你猜怎么样？完全跟量子力学的预言符合！

真的是你测得一个 EPR 对中的 A 是“上”的时候，B 就变成了“下”。本来是设计出来否定量子力学的，反而验证了量子力学的正确性。

3.6.3　泊松亮斑

这种事在科学史上屡见不鲜。19 世纪的时候，泊松主张光是粒子，菲涅耳主张光是波动。1818 年，菲涅耳计算了圆孔、圆板等形状的障碍物产生的衍射花纹。泊松指出，按照菲涅耳的理论，在不透明圆板的正后方中央会出现一个亮点。他认为这是不可能的，于是宣称驳倒了波动说。菲涅耳和阿拉果立即做实验，果然有个亮斑，如图 3-17 所示，波动说大获全胜。后人很有幽默意味地把这个亮点称为泊松亮斑。这正应了尼采的话：“杀不死我的，使我更强大！”

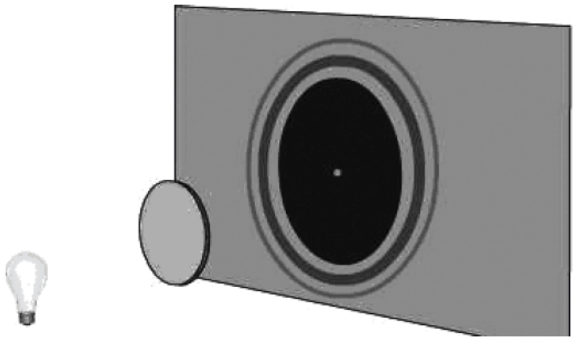


图 3-17　泊松亮斑

3.6.4　量子隐形传态是“嗖”的一声把人传过去的瞬间传输吗

EPR 现象既然是一个真实的效应，而不是爱因斯坦等人以为的悖论，人们就想到利用它。量子隐形传态（quantum teleportation）就是一个重要的应用，这是 1993 年按照量子力学设计出来的一种实验方案。

英文单词 teleportation 说的是隐形传态，在科幻小说和电影、电视剧中就表现为“嗖”的一声把人传过去的瞬间传输，所以配的都是传人的图片或视频。

可是，我们讲的是科学：量子隐形传态 实际能做到的是把一个粒子 A 的量子态传输给远处的另一个粒子 B，让 B 变成 A 最初的状态，传的是状态而不是粒子。根本传输不了一个大活人！

当然你可以说传人也是把人的所有原子的状态传到远处的另外一堆原子上，组合成一个同样的人。好，我没意见，只不过为了避免混淆，中国的科学家还是小心谨慎地把 teleportation 翻译成隐形传态，如图 3-18 所示。这个中文名称其实比英文名称好得多，准确而简练，反映出中文的优势。

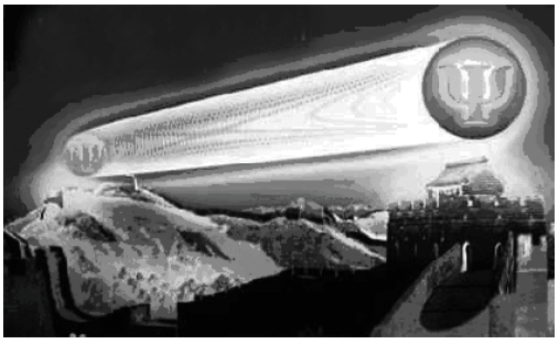


图 3-18　远距离量子隐形传态

1. 量子隐形传态的基本思路

量子隐形传态的基本思路是这样：让第三个粒子 C 跟 B 组成 EPR 对，而 C 跟 A 离得很近，跟 B 离得很远。让 A 跟 C 发生相互作用，改变 C 的状态，于是 B 的状态也发生了相应的变化。这时 A 和 C 这个两粒子集合的状态有四种可能，分别对应 00、01、10、11。B 的状态也相应地有四种可能，每一种可能都跟 A 最初的状态（即你想传输的目标状态）有一定程度的相似之处，可以通过某些量子力学的操作变成目标状态。

对 A 和 C 的整体做一次测量，A 和 C 就随机地突变到了 00、01、10、11 这四种状态中的某一个上，B 也突变到了相应的状态。现在你得到了一个两比特的 00、01、10 或 11，你可以把它理解为一个密码。把这个密码通过经典的通信手段（如电话、光缆）告诉 B 那边

的人，对 B 按照密码进行操作，就得到了 A 最初的状态。由此可见，量子隐形传态的基本元素包括中介粒子、密码和经典信道。

2. 凭这一招，信息传播速度就可以超光速吗

这里要澄清一个常见的误解。许多人把量子隐形传态当成了瞬间传输，不花时间就能传输到无限远处，然后高呼推翻了相对论。还有人以为凭这一招，信息传播速度就可以超光速，我们可以跟离地球 500 万光年的星球即时通话。这是完全错误的！

仔细看上面的流程，通过测量让各个粒子的状态突变确实可以不花时间，但是光凭这一步是无法得到目标状态的。为了知道对 B 要做什么操作才能得到目标状态，必须把那个两比特的字符串传过去，这就要通过经典的通信，而经典通信不能超过光速。由于有传输密码这一步卡着，所以量子隐形传态不能超过光速。

对这个结论有些沮丧吗？我得强调一句，成熟的科学理论不是这么容易推翻的。量子力学和相对论不是完全没有矛盾，但那是跟广义相对论有矛盾(引力问题)，狭义相对论跟量子力学还是很和谐的。量子隐形传态是个按照标准理论设计出来的方案，当然不会跟标准理论冲突。与其把它理解成一个推翻正统的革命家，不如把它理解成一个在现行体制下发挥奇思妙想的工艺大师。

还有一个常见的误解，是把量子隐形传态当成复制状态，然后就开始担忧两地同时出现一个自己，到底谁才是自己。这种理解也是错误的。仔细看量子隐形传态的流程，最终结果是 B 变成了 A 最初的状态，但 A 的状态也改变了。也就是说，任何时刻都只有一个粒子处于目标状态。如果要说这是复制，也是一种破坏性的复制，造出一个副本的同时就要把原本销毁。所以样品不会增多，只是从一个地方转移到了另一个地方而已。

总而言之，量子隐形传态是以不高于光速的速度、破坏性地把一个粒子的未知状态传输给另一个粒子。打个比方，用颜色表示状态，A 粒子最初是红色的，通过隐形传态，我们让远处的 B 粒子变成红色，而 A 粒子同时变成了绿色。但是我们完全不需要知道 A 最初是什么颜色。无论 A 是什么颜色，这套方法都可以保证 B 变成 A 最初的颜色，同时 A 的颜色改变。

量子隐形传态是在什么时候实现的？答案是 1997 年，当时潘建伟在奥地利因斯布鲁

克大学的蔡林格教授组里读博士，他们在《自然》上发表了一篇题为《实验量子隐形传态》的文章，潘建伟是第二作者。前面已经讲过，这篇文章后来入选了《自然》杂志的“百年物理学21篇经典论文”，跟它并列的包括伦琴发现X射线、爱因斯坦建立相对论、沃森和克里克发现DNA双螺旋结构等，这个阵容相当强大。当然，量子隐形传态的重要性不如那些神级成果，不过也已经相当了不起了，尤其是在基础科学已经很久没有革命的当代。

第4章

量子信息脸谱

最近40年，微电子产业一直遵循着摩尔定律的预测持续、高速发展。随着技术的进步，器件集成度越来越高，芯片上的晶体管数目越来越多，单个晶体管尺寸越来越小。可以说当前半导体芯片的发展已经接近尺寸上的物理极限，摩尔定律的时代即将终结，急需发展新的计算原理和新的器件架构来满足不断增长的计算需求。

在此背景下，各国科学家大力研究量子力学规律，发展量子计算与量子信息技术，以期研制出可替代传统计算机的实用化量子计算机，实现超高量子并行的超级计算能力。

量子计算机通过叠加和纠缠的量子现象来实现计算能力的增长。量子叠加使量子比特能够同时具有0和1的数值，可进行同步计算。每增加一量子比特，运算性能就翻一倍。

4.1 什么是量子信息

4.1.1 量子信息三兄弟

今天人们使用的计算机通过操作具有两种状态的位元(0或1)进行工作。量子计算机不只依靠两种状态。它们将信息编码为量子比特。量子比特可以是1或0，也可以是某种叠加态：即同时是1、0或两者之间的某个值。量子比特由一组原子实现，它们协同工作起到计算机内存和处理器的作用。因为量子计算机可以同时包含这几种状态，所以它可能比当今功能最强大的超级计算机还要强大数百万倍。

1. 量子比特

量子计算机的基本元件是量子比特，根据量子力学的基本原理，一量子比特可以同时有两种状态；二量子比特则可以同时表示 4 种状态；三量子比特可以同时表示 8 种状态等。随着量子比特数目的增加，其运算能力也呈指数级增加。当然，这其中也面临着一定的困难。测量或者观测一量子比特的行为可能会剥夺其计算潜力。于是，研究人员使用量子纠缠来获取信息。

2. 量子纠缠

在量子纠缠中，粒子被连接在一起，测量其中一个粒子的属性便可以直接揭示另一个粒子的相关信息，不管这两个粒子相距多远，如图 4-1 所示。但是，如何进一步高效地扩展纠缠的量子比特数目并让其维持这种纠缠状态，正是量子信息研究领域遭遇的严峻挑战。

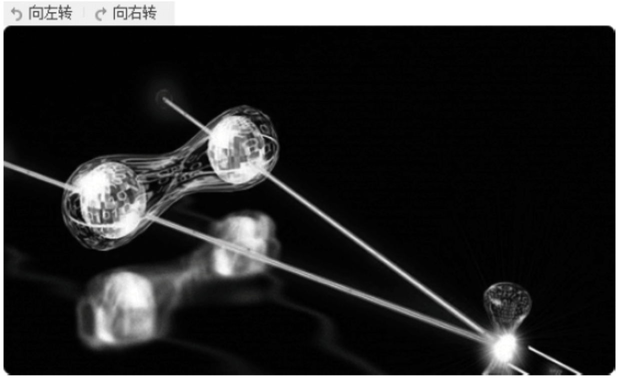


图 4-1　量子纠缠

3. 量子平行

一量子重叠态运行一量子比特同时存储 0 和 1。两量子比特能同时存储所有的 4 个二进制数。三量子比特能存储 8 个二进制数 000、001、010、011、100、101、110 和 111。300 量子比特能同时存储 2^{300} 个数字。这甚至多于宇宙中的原子数。

这表明了量子计算机的威力：只用 300 个光子（或者 300 个离子等）就能存储比这个宇宙中的原子数还多的数字，而且对这些数字的计算可以同时进行，如表 4-1 所示。

表 4-1 量子计算机的威力

量子比特数	同时存储数字的数目	可存储总数
1	(0 和 1)	$2^1=2$
2	(0 和 1)(0 和 1)	$2\times2=2^2=4$
3	(0 和 1)(0 和 1)(0 和 1)	$2\times2\times2=2^3=8$
⋮	⋮	⋮
300	(0 和 1)(0 和 1)…(0 和 1)	$2\times2\times\cdots\times2=2^{300}$

4.1.2 量子信息学

量子信息学就是以量子力学为基础，重新审视主流的计算和通信理论及其实现技术的尝试，之所以用尝试这个词，是因为这个学科的建立还是在向经典信息理论妥协的结果。

今天量子信息学在其智力的触角能伸到的地方已经取得了一些成果，其中容易理解的是量子比特的概念和隐形传输的通信技术。

在经典信息论中，信息量的基本单位是比特，一个比特代表经典二值系统(0,1)的一个取值的信息量。量子信息学中，基本单位是量子比特，量子比特是一个双态量子系统，这里的双态指的是两个线性独立态。在量子信息中，用作量子比特实现的双态系统就是光子。爱因斯坦是第一个认识到电磁辐射是以量子形式进行的，而且是以量子形式传播的。

掌握了量子比特的概念，其实就获得了一个更广阔的物质财富效应，可以实现在比特领域无法想象的操作。

量子隐形传态技术就是在新兴的通信领域，利用量子纠缠现象，可以实现不发送任何量子比特而把量子比特的未知态(即这个态包含的信息)发送出去。这样的结果，就是张三所拥有的“笑态＝笑容＋滑稽动作＋搞笑服装”，从张三处消失，并经过一个延迟(经典通信和李四的操作时间)，出现在李四那里。张三位置不动，李四位置也没有动，动的只是张三拥有的“笑态”，在李四处复活了。这在中国古代学术领域称为“遁术”。

与小说中称为“远距取物”不同的是，这只能称为“远距送物”，时间上送在先，复活在后。特别需要指出的是，上面的解说还受到线性的局限，理论上可以借助量子的隐形传态技术，传输任意复杂的量子态，包括这些态的组合。例如，量子密钥分配等超乎经典信息论可以理解的人间奇迹。

实际上，早在19世纪和20世纪之交时，物理学就完成了从牛顿力学向量子力学的转型。遗憾的是，世界如故，各个国家的教学与考试试题全部建立在经典数学和力学之上。

4.2 量子比特不是比特币

4.2.1 比特币

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通时各个环节的安全性。

P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。

比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

比特币可以用来兑现，可以兑换成大多数国家的货币。使用者可以用比特币购买一些虚拟物品，如网络游戏当中的衣服、帽子、装备等，只要有人接受，也可以使用比特币购买现实生活当中的物品，甚至病毒软件也要求受害者用比特币支付赎金。

美国西维吉尼亚州民主党参议员乔·曼钦2014年2月26日向美国联邦政府多个监管部门发出公开信，希望有关机构能够就比特币鼓励非法活动和扰乱金融秩序的现状予

以重视，并要求能尽快采取行动，以全面封杀该电子货币。

2017 年 1 月 24 日中午 12:00 起，中国三大比特币平台正式开始收取交易费。随后国家机构要求中国比特币平台停止运营。

4.2.2　量子比特

参照香农(Shannon)信息论中比特描述信号可能状态的特征，量子信息中引入了量子比特的概念。量子比特的英文名字为 quantum bit，简写为 qubit 或 qbit。

1983 年，Stephen wiesner 在他量子货币的提案中第一次引入了量子比特的概念。量子比特这个术语的问世只是因为它同古代的一种长度测量单位腕尺(cubit)的发音相似。在量子计算中，作为量子信息单位的是量子比特，量子比特与经典比特相似，只是增加了物理原子的量子特性。

1. 量子比特的基本原理

这一部分我们会阐述二进制、二进制序列和对二进制序列的操作。

我们首先来看计算机是怎么保存数据的。计算机中，用 0 和 1 二进制序列保存数据。抽象来看，二进制 0 和 1 分别代表了系统的两种状态。也就是说，我们只要能够找到一个有两个可以区分的状态的系统，就可以抽象地实现计算机的二进制。因此，我们首先讨论如何在系统中实现二进制。

在经典计算机中，0、1 由不同的电压实现，0 代表低电压信号，1 代表高电压信号。在量子力学中，我们有很多天然的双态系统来实现这种两个可区分的状态(不需要太纠结量子力学的态表示什么)。比如自旋 1/2 系统，这在量子力学中对应自旋向上/向下两种状态的系统；或者更经典的光子的极化，例如，一束光具有不同的偏振状态(如左旋/右旋偏振光)。总之，我们能够在量子力学中找到实现二进制的系统。

在实现二进制之后，下一步是需要得到二进制序列。

在经典计算机中，二进制序列由一个高低电压交错的脉冲实现。例如，001 对应于一个低电压-低电压-高电压的信号。在量子力学中，通过纠缠态实现二进制序列。具体而言，如果某个光子处于态上，可以把这个光子和其他光子纠缠起来得到一个 N 光子纠缠

态，这样就实现了一个二进制的序列。

在这里，量子世界和经典世界出现了不同。

在经典世界中，我们只能同时拥有一个状态。例如，如果我们拥有了 001 态，就不能同时拥有 010 态，这是因为两个态的电压会叠加，如果同时拥有这两个态，我们只能够得到 011 态。

在量子世界中，可以得到叠加态。具体来说，系统的状态可以同时处于态。其中叠加系数 a、b 的模方表示在测量中得到相应态的概率。

和经典比特有一个状态 0 或者 1 相似，量子比特也有一个状态，量子比特的两个状态可以表示为 $|0\rangle$和 $|1\rangle$。它们分别对应的是经典比特中的 0 和 1，记号 $|\ \rangle$称为 Dirac 记号，在量子力学中表示状态。

经典比特和量子比特的区别在于，量子比特的状态可以落在 $|0\rangle$和 $|1\rangle$之外。量子比特可以是状态的线性组合，常称为叠加态，例如 $|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$，其中 α 和 β 是复数。换句话说，量子比特的状态是二位复向量空间中的向量。

经典计算机通过经典的比特（bit）执行操作，这些比特不是 0 就是 1，而量子计算机借助的是量子比特。量子比特可被表示为绕核旋转的电子和光子，如图 4-2 所示。光子的偏振态和电子的自旋态可用$|1\rangle$和$|0\rangle$分别表示。

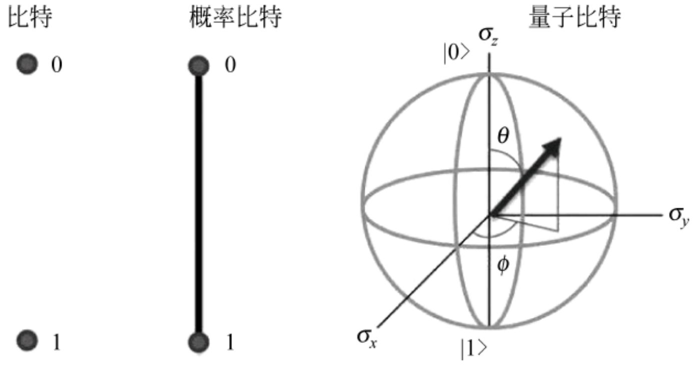


图 4-2　量子比特

量子比特被定义为一对指向单位球面中一个点的复杂向量。一般来说，直指上方（正

轴)的量子比特表示为列向量|0〉,指向下方(负轴)的量子比特为行向量|1〉。

2.量子比特的实现

目前,Google、Microsoft、IBM、Intel 等科技公司都已经布局量子计算的研究。IBM 公司宣称已成功开发出一台 50 量子比特的原型机;Google 公司量子硬件负责人约翰·马丁尼斯则透露 Google 公司已拥有 22 量子比特的芯片;中国也在 2017 年 5 月初发布了世界首台超越早期经典计算机的光量子计算机,成功实现了 10 超导量子比特纠缠,预计不久的将来可以实现操纵 20 超导量子比特。

优质的量子比特实现方式一般需要满足几项特定“指标”的要求,如较为容易的物理载体的实现方式、容易的初态制备和操作、较长的相干时间等。

目前量子比特的实现方案主要包括超导回路、囚禁离子、半导体量子点、金刚石空位、拓扑任意子和光子等,其中每一种技术都有自己的优点和缺点,未来最终路线尚不明确。上述方案中,半导体量子点方案最具核心优势,其可利用现有半导体工艺基础开发、操作速度快、易于实现高密度集成,从而吸引了众多研究机构的关注。

实现量子计算的主要障碍是用于计算的量子态难以保持,就是常说的相干时间短。半导体量子点可以利用现有的半导体工艺实现,从而可以基于现有技术较为平滑地从经典的半导体芯片过渡到量子芯片。

4.3　量子信息的身世

4.3.1　量子信息的源头

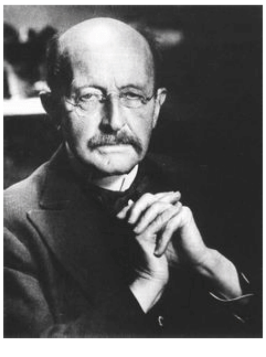


图 4-3　普朗克

1900 年,普朗克首次提出量子的概念,用来解决困惑物理界的“紫外灾难”问题。普朗克的肖像如图 4-3 所示。

当时的物理界,包括普朗克本人,都讨厌量子这个怪物,千方百计地想要将它消化在经典物理的世界之中,但却屡试不果。唯有爱因斯坦独具慧眼,他认为光辐射不仅在于与物质相互作用时的能量是一份一份的,光辐射的能量本身就是“量子化”的,一份

能量就是光能量的最小单元，后来称之为光量子，或简称光子。

普朗克假定，光辐射与物质相互作用时其能量不是连续的，而是一份一份的，一份“能量”就是所谓的量子。从此“量子论”就宣告诞生。

法国年轻的博士生德布罗意在爱因斯坦光子概念的启发下提出：既然看似波动的光辐射，具有粒子特性，那么像电子这类看似粒子的物质，也应具有波动性。这就是“德布罗意物质波”的概念，由此引发后继大量理论与实验研究，证实所有微观粒子都同时具有波动性和粒子性。这些奇异特性的微观粒子构成“量子世界”，遵从量子力学的运动定律。

德布罗意的肖像如图 4-4 所示。

图 4-4　德布罗意

随着科学技术的发展，人们认识到量子世界不仅限于微观和单个粒子，某些宏观尺度下的多粒子系统也遵从量子力学规律。例如，玻色-爱因斯坦凝聚（BEC），当原子聚合的温度足够低时，所有处于不同状态的原子，会突然聚集在同一个尽可能低的能量状态上，其行为就像一个“放大”的玻色子，遵从量子力学规律。

我们按物理运动规律的不同，将遵从经典运动规律（牛顿力学、电磁场理论）的那些物质所构成的世界称为经典世界，将遵从量子力学规律的那类物质所构成的世界称为量子世界。量子就是量子世界中物质客体的总称，它既可以是光子、电子、原子、原子核、基本粒子等微观粒子，也可以是 BEC、超导体等宏观尺度下的量子系统，它们的共同特征是必须遵从量子力学的规律。

举一个例子说明量子与经典世界的本质区别。经典世界的特点是物体的物理量、状态在某个时刻是完全确定的：晶体管要么导通，要么关闭，完全确定，即经典信息要么是 0，要么是 1，毫不含糊。量子世界中，客体的物理量则是不确定的、概率性的，而且这种不确定性与实验技术无关，是量子世界的本质特征，无法消除。这个特征体现在量子力学中重要的量子态叠加原理上。

量子态是科学家引进量子力学中用来描述量子系统的状态，其运动规律是薛定谔方程。

量子态又称为波函数或几率幅，是一个描述粒子的量子行为的复函数，它没有与任何经典世界对应。虽然人们并不喜欢量子世界这种描述，因为它与我们所熟悉的经典世界截然不同，但一百多年来所有实验都证实了量子力学的所有预言，人们不得不承认这种描述是正确的。

著名物理学家费曼说："量子力学的奥妙之处就是引入几率幅。"费曼的肖像如图 4-5 所示。

正是量子态的种种奇异特性导致量子信息技术的性能可以突破经典物理的极限，为人类开拓新一代的信息技术。

事实上，量子力学的所有奇异特性正是源于几率幅。当然，近百年来对量子力学争论不休也在于这个几率幅（量子态）。

图 4-5　费曼

4.3.2　量子信息技术的发展

量子信息技术（quantum information technique）是量子物理与信息技术相结合发展起来的新学科，主要包括量子通信和量子计算两个领域。量子通信主要研究量子密码、量子隐形传态、远距离量子通信技术等；量子计算主要研究量子计算机和适合于量子计算机的量子算法。

1. 量子计算

1965 年，Intel 公司的创始人之一戈登·摩尔针对电子计算机技术的发展提出了"每 18 个月计算能力翻倍"的摩尔定律。然而，由于传统技术的物理局限性，这一能力或将在未来 10～20 年达到极限。据保守估计，2018 年芯片制造业就将步入 16nm 的工艺流程，业内专家则认为，16nm 制程已经是普通硅芯片的尽头。事实上，当芯片的制程小于 20nm 之后，量子效应将严重影响芯片的设计和生产，单纯通过减小制程将无法继续遵循摩尔定律，而突破的希望恰在于量子计算。

从理论上讲，一个 250 量子比特（由 250 个原子构成）的存储器，可能存储的数达 2^{250}，比现有已知宇宙中全部原子数目还要多。无论在基础理论还是在具体算法上，量子计算都是超越性的。因此，对量子计算的相关研究及量子计算机的具体研制已成为世界科学

领域最闪亮的“明珠”之一。

例如，美国国防部对此就给予高度重视，国防部高级研究计划署（DARPA）专门制订了名为“量子信息科学和技术发展规划”的研究计划，其对外公开宣称的目标是，若干年内要在核磁共振量子计算、中性原子量子计算、谐振量子电子动态计算、光量子计算、离子阱量子计算及固态量子计算等领域取得重大研究进展。

2. 量子密码

目前的密码大都采用单项数学函数的方式，应用了因数分解或其他复杂的数学原理。例如，在目前互联网上比较常用的 RSA 密码算法，就是应用因数分解的原理。因为要计算两个大质数的乘积很容易，但要将乘积分解回质数却极为困难，这就使得密码很难被破解。

然而，美国科学家 Shor 却提出了“量子算法”。他利用量子计算的并行性，可以快速分解出大数的质因子，这意味着以大数因式分解算法为根基的密码体系在量子计算机面前不堪一击。

差不多同时，另一个著名的量子算法——量子搜寻算法也被提出。用该方法攻击现有密码体系，经典计算需要 1000 年的运算量，量子计算机只需小于 4min，从而使传统密码领域遭遇前所未有的挑战，以致有科学家宣称：“其意义不亚于核武器……一旦有些国家拥有了量子计算机，而另一些国家却没有，当战争爆发时，这就犹如一个瞎子和一个睁眼的人在打架一样，对方可以把你的东西看得清清楚楚，而你却什么都看不到。”

当然，量子计算机的出现虽然会对传统密码产生颠覆，但是量子信息同时也提供了一个守护神，即一种理论上无法破解的密码——量子密码。由于采用量子态作为密钥，具有不可复制性，因而无破译的可能，量子密码的出现也因此被视为“绝对安全”的回归。世界各国纷纷将其纳入国防科技发展战略之中。例如，美国洛斯阿拉莫斯国家实验室就在研究量子局域网的密码体系和自由空间量子密码。此外，英国国防部及欧盟各国也启动了类似的量子密码研究计划。

3. 量子通信

这个世界上真的存在“超时空隧道”吗？对此，科学家给出的答案是，这一说法今天看

来依然不无夸张，但与量子纠缠密切关联的量子态隐形传输则正在变为现实。

通俗而言，两个相距遥远的陌生人不约而同地想做同一件事，好像有一根无形的线绳牵着他们，这种神奇现象可谓“心灵感应”。与此类似，量子纠缠是指在微观世界里，有共同来源的两个微观粒子之间存在纠缠关系，不管它们距离多远，只要一个粒子的状态发生变化，就能立即使另一个粒子的状态发生相应变化。量子通信正是利用量子纠缠效应进行信息传递的一种新型通信方式。

在时空方面，量子通信为基于卫星量子中继的全球化通信网奠定了可靠基础。德国物理学家正在利用量子纠缠效应打造量子互联网，其研究人员称：“我们已经实现了第一个量子网络原型，在节点之间完成了量子信息的可逆交换。此外，还可以在两个节点之间产生远程纠缠，并保持约100μs……未来人们通过它不仅可以进行远距离的量子信息沟通，而且还将使大型量子互联网完全实现成为可能。”

显然，这一量子通信技术在军事应用方面有着无与伦比的广阔前景，量子隐形通信系统将建立在各类作战指挥控制体系之间和各种侦察预警系统、主要作战平台以及量子微空间武器系统之中，构建出量子信息化战场的通信网络，以其超大信道容量、超高通信速率等特性，在未来的信息化战争中扮演无可替代的角色。因此，近年来，美国国防部高级研究计划署启动了多项量子通信方面的相关研究计划。英国、德国、日本等国也都将量子通信技术纳入议程，对其开展了广泛的探索。

日前，我国自主研发的“墨子号”卫星在酒泉卫星发射中心发射，首次实现卫星与地面之间量子通信连接。自此，量子通信这一前沿科技开始走入大众视线。

量子通信中有三项核心技术，分别是单光子源技术、量子编码和传输技术、单光子检测技术。大量研究已经证明使用单光子源的量子通信是绝对安全的，并且具有很高的效率。由此可见，理想的单光子源是量子通信的基础，其特性的研究具有很高的价值。

量子通信的信道有光纤信道和自由空间信道两种，无论采用哪种信道进行实验，单光子源的质量都是影响整个通信过程安全性的重要因素。

4.3.3　小有小的规矩——量子编码定理和量子编码方案

量子编码定理(quantum coding theorem)是量子通信系统的基本定理。

1. 量子信源编码定理

量子信源编码定理：量子信源以概率 P 发送密度算符为 p 的量子态，表示信源的总密度算符。

量子信源编码定理表明，如果所有 p 均限制为纯态，则冯·诺依曼熵确定了表征这个量子系统的信息所需的最小量子比特数。若 p 为混合态，则相对冯·诺依曼熵确定了所需的最小量子比特数。

2. 量子信道编码定理

量子信道编码定理：在量子信息中，根据不同的辅助资源和通信用途，量子信道有如下几种不同的容量。

（1）经典容量 c。等于通过此量子信道可靠地传送经典比特的最大速率。

（2）量子容量 Q。指通过信道完全可靠地传送量子比特的最大速率。

（3）经典辅助量子容量“Q:”。指在通信双方无限制的经典通信辅助下，通过信道完全可靠地传送量子比特的最大速率。

（4）纠缠辅助经典容量 CE。指在通信双方拥有无限制的事先分享的量子纠缠的辅助下，通过此信道可靠地传送经典比特的最大速率。

3. 量子编码方案

国际上公认的主要的三种量子编码方案是量子纠错码、量子避错码和量子防错码。

量子态不可克隆原理指明了环境不可避免地破坏量子的相干性。这个消相干问题，会使量子计算机运行失效，因此，长期以来量子计算机一度被认为不可进入实际应用。解决量子的消相干问题是取得突破的关键。

为了攻克这一世界性难题，中国科学技术大学郭光灿教授和他的课题组通过实验发现，量子态在超辐射的条件下会发生集体效应，能在消相干的环境下保持其相干性，这一研究成果被国际学术界称为“无消相干子空间理论”。

量子计算的编码问题，一直被认为是克服消相干最有效的方法。郭光灿教授的研究小组运用他们的“无消相干子空间理论”，在国际上首创了“量子避错编码原理”，从根本上解决了量子计算中的编码错误造成系统计算误差问题。

4.4　这个“比特”和那个“比特”不一样

在量子力学中，有一条原理称为叠加原理：如果有两个状态是一个体系可以处于的状态，那么这两个状态的任意线性叠加也是这个体系可以处于的状态。这样的体系称为量子比特。

两个状态的线性叠加有无穷多个，因此，一量子比特就是一个有无穷多个状态的体系。打个比方，传统的比特相当于“开关”，只有开和关两个状态，而量子比特相当于“旋钮”，是连续可调的，有无穷多个状态。量子比特向左转或向右转，如图4-6所示。

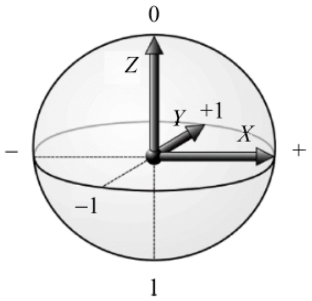


图4-6　量子比特向左转或向右转

显然，旋钮包含的信息量比开关大得多。用这样的量子比特组合成量子计算机，它肯定可以做到所有的传统计算机能做到的事，还有可能做到一些传统的计算机做不到的事。这些传统计算机做不到的事，就是量子计算机的价值所在。

4.4.1　风光无限“大哥大”——经典比特

比特由英文bit音译而来。

1. 信息量的度量单位

（1）比特是计算机专业术语，是信息量单位。二进制数的一位所包含的信息就是一比特，如二进制数0100就是4比特。

（2）二进制数字中的位，信息量的度量单位，为信息量的最小单位。数字化音响中用电脉冲表达音频信号，1代表有脉冲，0代表脉冲间隔。如果波形上每个点的信息用4位一组的代码表示，则称4比特，比特数越高，表达的模拟信号就越精确，对音频信号的还原能力越强。

2 比特的概念

二进制数系统中，每个 0 或 1 就是一个比特，比特是数据存储的最小单位。其中，8 比特就称为一个字节(Byte)。计算机中的 CPU 位数指的是 CPU 一次能处理的最大位数。例如，32 位计算机的 CPU 一次最多能处理 32 位数据。

bit 是 binary digit(二进制数)的缩写，是数学家 John Wilder Tukey 提议的术语。这个术语第一次被正式使用，是在香农著名的 *A Mathematical Theory of Communication* 论文中。

由于转换成二进制后长度会发生变化，不同数制下一位的信息量并不总是一个二进位，其对应关系为对数关系。例如，八进制的一位数字，相当于 3 个二进位。除二进位外，在计算机上常用的还有八进制、十进制和十六进制等的八进位、十进位和十六进位等。

各种进制的名字缩写及数字含义如表 4-2 所示。

表 4-2　各种进制的名字缩写及数字含义

名字(十进制)	缩写	次方(十进制)	名字(二进制)	缩写	次方(二进制)
Kilobit	kbit	10^3	kibibit	Kibit	2^{10}
megabit	Mbit	10^6	mebibit	Mibit	2^{20}
gigabit	Gbit	10^9	gibibit	Gibit	2^{30}
terabit	Tbit	10^{12}	tebibit	Tibit	2^{40}
petabit	Pbit	10^{15}	pebibit	Pibit	2^{50}
exabit	Ebit	10^{18}	exbibit	Eibit	2^{60}
zettabit	Zbit	10^{21}	zebibit	Zibit	2^{70}
yottabit	Ybit	10^{24}	yobibit	Yibit	2^{80}

4.4.2 领跑下一代——量子比特

在量子计算中，作为量子信息单位的是量子比特，量子比特与经典比特相似，只是增加了物理原子的量子特性。量子计算机的物理结构是纠缠态原子自身的有序排列，量子比特在系统中表示状态记忆和纠缠态。

量子计算是通过对具有量子算法的量子比特系统进行初始化而实现的，这里的初始化指的是把系统制备成纠缠态的一些先进的物理过程。在两态的量子力学系统中量子比特用量子态来描述，这个系统在形式上与复数范围内的二维矢量空间相同。

两态量子力学系统的例子是单光子的偏振，这里的两个状态分别是垂直偏振光和水平偏振光。在经典力学系统中，一个比特的状态是唯一的，而量子力学允许量子比特是同一时刻两个状态的叠加，这是量子计算的基本性质。

从物理上来说量子比特就是量子态，因此，量子比特具有量子态的属性。由于量子态的独特量子属性，量子比特具有许多不同于经典比特的特征，这是量子信息科学的基本特征之一。

目前，量子比特还没有一个明确的定义，不同的研究者采用不同的表达方式。例如，从物理学的角度，人们习惯于根据量子态的特性称为量子比特（qubit 或 qbit）、纠缠比特（ebit）、三重比特（tribit）、多重比特（multibit）和经典比特（cbit）等。这种方式让人眼花缭乱，并且对量子比特的描述要根据具体的物理特性来描述。为了避免这些问题的困扰，本书从信息论的角度对量子比特做出统一的描述。

4.4.3　量子比特叠罗汉

量子纠缠是什么？

关于量子纠缠的比喻有很多。我们再补充一个：“在美国的女儿生下孩子那一瞬间，远在中国的母亲就变成了姥姥，即便她自己还不知道。之所以她是姥姥别人不是，而且她一定会成为姥姥，就是因为她和女儿之间有一种‘纠缠’关系。”

1. 量子比特的实现

目前，量子信息和量子计算实验研究中，用到的量子比特实现方法各种各样。归纳起来，承载量子比特的物理实体有光子、光学相干态、电子、原子核、光学栅格、约瑟夫森结、单个充电的量子点对和量子点。

对光子而言，可用偏振态、光脉冲中的光子数和光子出现的时间来表示量子比特 0 和 1。

对于光学相干态，可用其不同分量表示不同的量子比特。

对于电子，可用其自旋方向或电子的有无来表征量子比特。

对于原子核，可采用不同的核自旋方向表示不同的量子态。

对于光学栅格，可采用原子的自旋方向表示量子比特。

对于约瑟夫森结，可采用超导量子岛(island)是否带电、超导流(flux)的电流方向或超导相位(基态/激发态)来表示量子比特。

对于单个充电的量子点，可用电子的位置表示量子比特。

对于量子点，可用量子点的自旋方向表示量子比特。

2.量子测量

在量子力学中，“测量”需要有较严谨的定义，所以，特别称之为量子测量。量子测量不同于一般经典力学中的测量，量子测量会对被测量子系统产生影响，例如，改变被测量子系统的状态；处于相同状态的量子系统被测量后可能得到完全不同的结果，这些结果符合一定的概率分布。量子测量是量子力学解释体系的核心问题，而量子力学的解释还没有统一的结论。除了实验物理上的考量之外，量子测量涉及的层面也包括哲学观点。

与经典物理中的测量不同，量子测量不是独立于所观测的物理系统而单独存在的，相反，测量本身是物理系统的一部分，所做的测量会对系统的状态产生干扰。

4.4.4 谨防“李鬼”！基于量子比特原理才叫量子产品

随着我国量子通信技术的快速发展，量子技术产业化的步伐也在加快。尽管取得的成绩有目共睹，但其中“李鬼”横行的现象也不少，如量子水、量子鞋垫、量子水杯等产品充斥网络，一时间，关于量子产品的讨论也成为舆论关注的焦点。

到底该如何定义量子产品？

针对这些现象和疑问，答案是，所有基于量子比特原理的产品才能叫量子产品，量子比特是由一个光子或原子的能级状态所表征，是非常微观的东西，不可能形成网上卖的能看得见摸得着的日用品。

多名受访者认为，对于借用量子的概念，打着高科技、先进等噱头高价出售的“量子产

品”，消费者要谨慎辨别。但在量子科技产业化推进的过程中，我们也不可因噎废食，对于量子产业的新突破、新应用要持客观和正面的态度。

1. 量子很“微观”，极难形成可感知产品

一般意义上，量子就是量子世界中物质客体的总称，它既可以是光子、电子、原子、原子核、基本粒子等微观粒子，也可以是BEC、超导体等宏观尺度下的量子系统，它们的共同特征就是其性质必须由量子力学来描述。

量子很难形成能被具体感知的产品，量子是比较微观的东西，主要是利用量子的特性形成产品，而不是直接用量子形成产品。

网络上的量子产品在宣传中称，因量子具有微粒子特性和高频共振特性，量子产品的产生是在物质原有频率上再加载一种微观世界看不到的能量波频，称为量子能量波，具有了量子能量波的产品即为量子产品。

根本不存在量子能量波这个定义，这样的产品纯粹属于忽悠。量子的特性是量子叠加和量子纠缠，对量子特性应用比较多的是量子计算和量子通信。

目前，在世界上，美国的量子计算处于领先水平，而中国的量子通信技术则比较领先。量子计算是矛，量子通信是盾。量子密钥技术是目前唯一已经被证明能够对抗量子计算机超强计算能力的密钥体系。

目前，量子计算机技术还不成熟，被广泛应用的是量子通信技术。而现在用于应用的量子通信，本质上是量子密码，是用来传递密钥，对信息进行加密。

2. 现阶段量子应用集中于加密和计算

量子力学诞生至今经历了两次革命：第一次量子革命，开发出了激光、半导体等新型的经典器件，这些器件遵从经典物理规律；第二次量子革命则是直接开发基于量子特性本身的量子器件，这些器件遵从量子力学规律，它以量子态（量子比特）为单元，信息的产生、传输、存储、处理、操控等全都基于量子力学规律，是地道的量子器件，称为量子信息技术。

目前，量子革命尚在发展阶段，量子计算机出来后，第二次量子革命才算完成，所有基于量子比特的产品才能叫量子产品，目前很多量子产品是在炒作量子概念。

目前，量子通信是量子领域最前沿的技术，但也只是用到了量子的一部分特性，量子

通信用的是量子的不可克隆和测不准原理，保证信息传输过程的安全。

随着全球信息安全问题越来越严重，量子通信产业被广泛关注。作为与传统通信相结合的一种高效安全通信方式，量子通信不仅可用于军事、国防等领域，还可以应用于金融、政务等行业。

近年来，量子通信已逐步从理论走向实验，技术取得重大突破，研发出了一系列产品。

我国量子通信产业化目前还处于非常初级的阶段，市场化机制未形成，量子通信的发展还是靠国家政策推动，市场竞争不充分，尚未开发出一款真正的产品，让人们真实看到量子有什么用，能用在什么地方。

不管什么样的产品，背后一定是有数学和物理的基础知识和理论支撑，这就是网上的量子产品不可信的原因。

第5章

未来世界的大佬——量子计算

量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式。对照于传统的通用计算机，其理论模型是用量子力学规律重新诠释的通用图灵机。

如果把现在传统的电子计算机比作自行车，那么，量子计算机就好比飞机。量子计算机为何可以成为计算机界的“战斗机”？这与它的计算原理密切相关。

现有的电子计算机，一个物理比特只能存储一个逻辑态——或者0，或者1。而量子计算机利用的是量子的相干叠加原理，可以制备在两个逻辑态0和1的相干叠加态，换句话讲，一量子比特可以同时存储0和1。

这意味着什么呢？意味着量子计算机的处理能力将随着比特数的增加而呈指数级上升。量子计算机有 N 比特，就可以一次对 2^N 个数进行数学运算，相当于经典计算机算上 2^N 次。

量子计算的能力随可操纵的粒子数呈指数增长，这可以为经典计算机无法解决的大规模计算难题提供有效解决方案。

如果考虑分解300位大数，利用万亿次经典计算机需要15万年，利用万亿次量子计算机只需要1s。

据预测，2020年左右超导量子计算机就可以操纵50量子比特，到时就可以实现“量子称霸”，从而在处理一些特定问题的能力上超越经典计算机中计算能力最强的超级计算机。10年内量子计算机将可能实现对100个粒子的相干操纵，届时它处理特定问题的能力就可以达到目前全世界计算能力总和的百万倍。

5.1 量子计算

目前，我们的技术还无法实现真正意义上的量子计算机，因为添加更多的量子位和处理亚原子需要低于－269℃的低温环境。因此，Microsoft 公司通过量子模拟器模拟 40 量子比特的操作，通过 Azure 云计算资源进行扩展。

量子计算可解决专业的科学问题，如分子建模、高温超导体的产生、药物建模和测试、分子的选择以及有机电池的制造。对于看视频或写 Word 文档等一般用途的任务，它并不是最佳选择。

5.1.1 量子计算的发展历程

量子计算是最重要的后摩尔技术之一，拥有电子计算机无可比拟的超强计算能力。2012 年诺贝尔物理学奖颁奖委员会评价称，量子计算有望在 21 世纪里彻底改变人们的生活，正像传统计算机在 20 世纪中所做的那样。

1. 量子计算概念的提出

量子计算的概念最早由阿尔贡国家实验室的 Benioff 于 20 世纪 80 年代初期提出，他提出二能阶的量子系统可以用来仿真数字计算；稍后费曼也对这个问题产生兴趣并着手研究，1981 年，在麻省理工学院举办的计算物理第一届会议上，诺贝尔物理学奖获得者费曼在报告中指出，使用经典计算机难以有效模拟量子系统的演化。他首次提出量子计算机的概念，说明使用量子计算机能够对量子系统的演化进行有效模拟。

1985 年，牛津大学的 D. Deutsch 提出量子图灵机（quantum Turing machine）的概念，量子计算才开始具备了数学的基本型式。然而，上述的量子计算研究多半局限于探讨计算的物理本质，还停留在相当抽象的层次，尚未进一步跨入发展算法的阶段。

2. 量子计算中期发展

1994 年，麻省理工学院数学家 Shor 提出分解大数质因子的量子算法——Shor 算法，能够在多项式时间复杂度求解 RSA 密码体系中核心的大数质因子分解问题，与当前最好

的经典算法相比具有指数加速性能。

这个结论开启了量子计算的一个新阶段：有别于传统计算法则的量子算法(quantum algorithm)，它确实有其实用性，绝非科学家口袋中的戏法，从而掀起了国际上研究量子计算的第一轮热潮。

随后近20年，量子计算在物理实现、算法、程序设计等各个方向都取得许多重要进展。例如，2012年诺贝尔物理学奖授予了美国科学家大卫·温兰德和法国科学家塞尔日·阿罗什，表彰他们在测量和操控单量子系统方面做出的开创性的实验工作，被评价为：在利用量子物理效应构建超快量子计算机方面迈出了第一步。

自此之后，新的量子算法陆续被提出来，而物理学家接下来所面临的重要的课题之一，就是如何去建造一部真正的量子计算器，来执行这些量子算法。许多量子系统都曾被点名作为量子计算器的基础架构，如光子的偏振、腔量子电动力学、离子阱以及核磁共振等。截至2017年，考虑到系统的可扩展性和操控精度等因素，离子阱与超导系统走在了其他物理系统的前面。

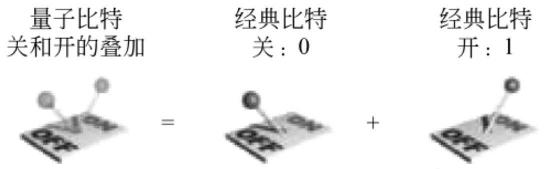
当前，量子计算领域快速发展，正迎来第二轮研究热潮。起因来自技术的不断进步，以及玻色采样量子模拟等非标准量子计算技术受到更多关注。中国、美国、欧盟、英国等国家和地区都在开展对量子计算的研究，Google、IBM、Microsoft等IT巨头也都纷纷成立量子计算实验室，与高校开展联合研究。相信在本次研究热潮中，量子计算将获得新一轮的重要突破。

5.1.2　量子计算的基本原理

量子计算是一种与经典计算完全不同的、基于量子比特的全新计算技术。图5-1解释了量子计算的基本原理。

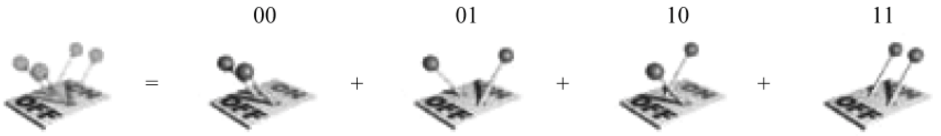
量子比特的载体遵循量子力学的规律，可以处于0和1的相干叠加态。也就是说，一量子比特可以同时包含0和1的信息。这种特性称为量子叠加，系统处于量子叠加的能力称为相干性。对叠加的量子比特进行操作，就同时完成了对0和1的操作。

这类似于传统计算机中的单指令流多数据流(SIMD)并行。不同之处在于，SIMD并

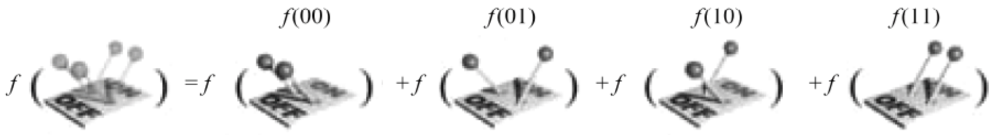


注：这里“+”指量子力学中的量子叠加，
不是四则运算中数的加法。
准确地说，是Hilbert空间中的矢量加法

(a) 1量子比特可以同时包含0和1的信息



(b) 2量子比特可以同时包含00、01、10和11的信息



(c) 对2量子比特的运算同时完成了对00、01、10和11的运算

图 5-1　量子计算的原理

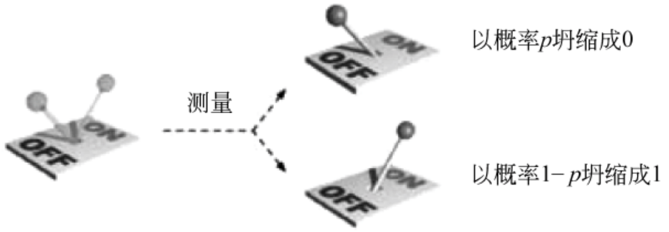
行需要 2 经典比特才能完成 0 和 1 的并行运算，而量子计算只需 1 量子比特就可以。

更重要的是，量子叠加所能同时表示的数随着量子比特数目的增加而指数增长。N 量子比特能同时包含 2^N 个数的信息，对这 N 量子比特的运算就同时完成了对 2^N 个数的运算。这种“超并行”的运算方式带来了量子计算的超强运算能力。

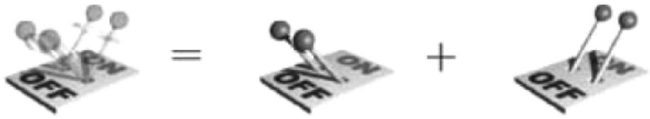
量子物理中充满了各种违背人类直觉的诡异现象，而它们恰恰是构造量子计算的基本要素。图 5-2 中展示了“让这个世界以概率方式运行”的测量和“拥有诡异超距作用”的量子纠缠。

图 5-2(a)中对叠加的量子比特进行测量，会改变叠加的量子比特，以概率的方式变为 0 或 1。爱因斯坦不接受用这种概率的运行方式(非决定论)，说“上帝不掷骰子”，但大量的物理实验都在不断验证量子物理的预言结果。

量子纠缠是一种特殊的量子叠加状态(称为叠加态)。图 5-2(b)中有二量子比特，将 00 和 11 叠加在一起。如果对这二量子比特进行测量，它们会坍缩到 00 或者 11。但是，



(a) 测量量子比特会导致其概率地变化成(坍缩)经典比特的状态



(b) 量子纠缠：一种特殊的叠加态，对这两个量子比特进行测量，
若第一个比特坍缩成0(关)，那么第二个比特也坍缩成0(关)；
若第一个比特坍缩成1(开)，那么第二个比特也坍缩成1(开)

(c) 量子纠缠的“超距”作用；
无论两个纠缠的量子比特相距多远，也会发生测量的关联坍缩现象

图 5-2　量子测量与量子纠缠

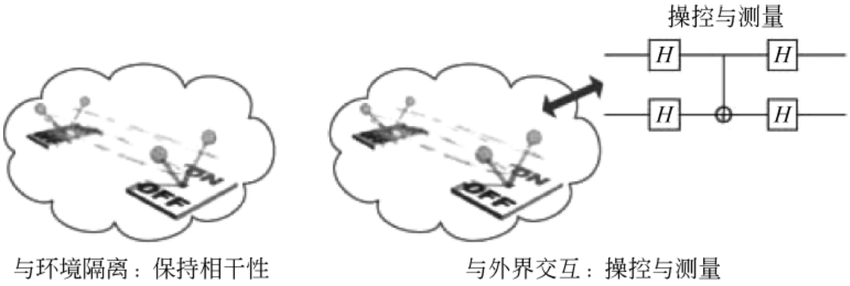
如果第一量子比特变成了 0,那么第二量子比特也一定会变成 0。

同样地,如果第一个变成 1,第二个也一定会变成 1。关键在于,无论这两个量子比特相距多远,即使一个在地球上,另一个在火星上,如果一个量子比特发生坍缩,另一个也会以关联的方式瞬时坍缩。图 5-2(c)显示了无论两个纠缠的量子比特相距多远,也会发生测量的关联坍缩现象。

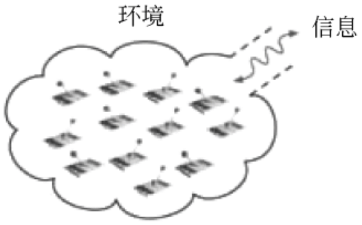
5.1.3　量子计算机的实现

如何实现量子计算机,是目前量子计算领域公认的最大挑战。图 5-3 解释了大规模量子比特系统面临的退相干问题。要保持量子系统的相干性,就需要让其与环境尽可能隔离,而计算所需的“操控与测量”本质上又是外界与量子系统的主动交互,“与环境隔离”

和“与外界主动交互”形成一对矛盾。



(a) 环境与系统进行信息交互(环境对系统进行测量)将破坏相干性
矛盾：保持相干性要与环境隔离；操控与测量要与外界主动交互



(b) 量子比特变多时，相干性控制困难，一旦环境对系统进行了测量
(发生了信息交互)，系统的相干性丢失，坍缩到没有叠加的状态

图 5-3　大规模量子比特系统面临的退相干问题

这种困难在大规模量子比特上变得更加突出,这也是量子效应很少在宏观系统中显现得重要的原因。例如,薛定谔的猫等人类生活的宏观尺度里,环境与系统的作用难以避免,“环境对系统的测量”使得系统很难处于叠加的量子态。

与此同时,一项非常重要的非技术挑战是物理学、计算机科学等多个学科的交叉合作。在电子计算机中,应对同一问题往往有多种解决方案。例如,针对器件的可靠性问题,可以在物理电路层改进,也可以在数据编码时引入纠错码,还可以在系统结构层增加多模冗余等纠检错机制。

现有的量子计算研究中,至少可以划分为量子算法、量子程序设计、量子计算机体系结构、量子计算物理实现等多个层次。这些层次的研究目前分布在不同学科,学科之间的交叉合作明显不足,尚有很大的发展空间。

量子算法是量子计算研究的重要推动力。20 世纪 90 年代,正是 Shor 算法的提出,

让人们认识到量子计算的巨大价值；现阶段，引起大家再次关注量子计算的原因之一，恰恰还是量子退火、玻色采样等量子算法或与其有关的研究。目前量子算法领域的重要进展包括隐含子群问题、搜索问题、量子模拟、量子漫步和线性方程组求解等。

软件是传统计算机的“灵魂”，量子软件和量子程序对于发挥未来量子计算机的强大计算能力也有着不可替代的重要作用。由于量子计算的一些独特性质，如量子信息的不可克隆性、量子纠缠等，传统电子计算机的软件理论与方法并不能直接运用于量子计算机。量子程序设计研究，不仅是为了开发量子计算机上的程序和软件，还能够让我们进一步理解和认识量子计算本身。

量子计算物理实现是当前的研究焦点，目前研究的物理体系包括光量子、量子点、离子阱、超导、冷原子、金刚石色心和核磁共振等。各种物理体系拥有各自的优缺点，究竟哪种体系是最佳的量子计算物理实现途径尚未可知。同时，有观点认为未来的量子计算机会是多种物理体系的混合，类似于经典计算机，CPU 用 CMOS 晶体管，内存 DRAM 用电容，硬盘用磁介质，光盘用光介质。

超导属于固态量子物理体系，采用现代微纳米加工技术，近年来发展迅速，受到广泛关注。拓扑量子计算是一种极其优美、全新的理论和实验方法，对局部扰动引起的退相干免疫，伴随马约拉那费米子等近期基础物理研究的突破受到越来越多的关注。

半导体量子点也属于固态量子物理体系，是最容易大规模集成的物理体系之一。

光子是“飞行量子比特(flying qubit)”，不仅可以作为量子处理单元的物理载体，还可以作为连接多个量子系统的桥梁，在未来的量子计算中占据着重要地位。

离子的相干时间非常长，离子阱也是研究最早和发展最快的物理体系之一。

5.1.4　光量子计算机

光量子计算机包含 3 个主要部分。

第一部分是单光子源，在零下 269℃的低温中，这个设备通过激光激发量子点，每次产生一个高品质的单光子，是国际上最高品质和最高效率的单光子源。

第二部分是超低损耗光量子线路。单光子通过开关分成 5 路，通过光纤导入主体设

备光学量子网络。

第三部分是单光子探测器，探测矩阵中得到的量子计算结果。

多粒子纠缠的操纵作为量子计算的核心资源，一直是国际角逐的焦点。在光子体系，利用量子点单光子源，通过电控可编程的光量子线路构建而成。

顾名思义，量子计算机需要对量子进行高精度调控，这需要极低的温度。目前发展最快的三大量子计算机体系中，光量子计算机可以在室温下运行，但要在零下 269℃的低温中产生单光子；超导量子计算机的 CPU 芯片可以在常温下展示，但它的真正运行必须在接近绝对零度（零下 273.15℃）的环境中进行；超冷原子量子计算机所需的低温是三者中最低的，最接近绝对零度。

量子计算机可以实用化，未来全世界会有很多台，但不需要家家都有。量子计算机可以和现有的经典计算机配合使用。以现有的手机终端为例，手机就是小型计算机，它要做成低温的量子计算机，会很难，也没有必要。但可以通过云计算平台，用手机把需要完成的计算任务送到云端，让后台的量子计算机来完成。

传统计算机能算好的问题，量子计算机不需要再去介入。量子计算机瞄准的，是传统计算机不能解决的难题，例如，玻色取样对经典计算机太难了，量子计算机在这方面就显得特别强大。

当量子计算机实用化以后，它能解决哪些实际应用领域的难题呢？

密码分析、气象预报、药物设计、金融分析、石油勘探、人工智能、大数据等，总之，那些需要超大计算量的难题，交给量子计算机就对了！

5.2 量子计算的黑白两道

5.2.1 白道：量子叠加性

这些内容我们已经在有关量子力学的一节里做好了准备，但是重要的事情说三次，下面再复习一下。

1. 量子纠缠和量子叠加原理

1）量子纠缠

量子纠缠是关于量子力学理论最著名的预测。它描述了两个粒子互相纠缠，即使相距遥远，一个粒子的行为也会影响另一个粒子的状态。当其中一个粒子被操作（例如量子测量）而状态发生变化时，另一个粒子也会即刻发生相应的状态变化。

量子纠缠意味着两个纠缠在一起的量子就像有心电感应的双胞胎，不管两个人的距离有多远，当哥哥的状态发生变化时，弟弟的状态也跟着发生一样的变化。

如果这两个光量子呈纠缠态的话，哪怕是数千米量级或者更远的距离，大家认为，还是会出现遥远的点之间的诡异互动。两个处于纠缠状态的粒子无论相距多远，都能“感应”对方状态，爱因斯坦称之为“幽灵般的超距作用”。科学家就可以利用这种效应将甲地某一粒子的未知量子态，在乙地的另一粒子上还原出来。

2）量子叠加原理

也就是说，量子有多个可能状态的叠加态，只有在被观测或测量时，才会随机地呈现出某种确定的状态。因此，对物质的测量意味着扰动，会改变被测量物质的状态。

这就好比孙悟空的分身术，一个孙悟空同时出现在多个地方，孙悟空的各个分身就像是他的叠加态。在日常生活中，人们不可能同时出现在两个地方，但在量子世界里，作为一个微观的客体，它同时出现在许多地方。

量子力学态叠加原理使得量子信息单元的状态可以处于多种可能性的叠加状态，从而导致量子信息处理从效率上相比于经典信息处理具有更大潜力。普通计算机中的2位寄存器在某一时间仅能存储4个二进制数（00、01、10、11）中的一个，而量子计算机中的2位量子位寄存器可同时存储这4种状态的叠加状态。随着量子比特数目的增加，对于n量子比特而言，量子信息可以处于2^n种可能状态的叠加，配合量子力学演化的并行性，可以展现比传统计算机更快的处理速度。

2. 量子叠加态

量子的态就是指粒子的在空间中的状态，如能量、自旋、运动、场等。量子的态可以用波函数描述，所以波函数又被称为态函数。

量子的态是可以线性叠加的，如双缝干涉，干涉光的波函数就是透过缝隙的两束光的波函数的叠加。还有比如电子的轨道叠加等，也可以用电子态叠加来解释。

叠加态是由几种本征态叠加在一起的粒子状态，这时这个状态是不确定的，只有当一个“测量”被进行的时候，才会呈现一个被测量的状态，可能是它的任何一种本征态。叠加态如图 5-4 所示。

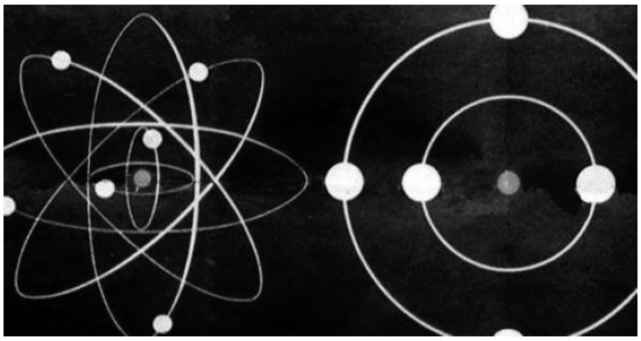


图 5-4　叠加态

简单来讲，量子叠加态就是一个事物，你在观察它之前它既是 a 也是 b，可同时处于这两种状态，一旦你观察了它，就只能是 a 或 b 一种状态了，举个例子，一枚硬币抛向天空落下来之后立刻用手盖住，此时硬币既可以是正面朝上也可以是背面朝上，但如果你一旦拿开手，看到了这一枚硬币，它就只能是一种状态了。

量子的这些特性听起来既特别又神奇，其实道理并不难，这是因为整个宇宙都是一团能量，量子纠缠中的粒子 a 和粒子 b 都处在这个能量团中，而且 a 和 b 本身也是这团能量的一部分，它们之间本来就是密切相关的所以，a 的状态改变会影响 b 的状态而且是瞬间的。

这样一来量子的叠加态就更好解释了，整个宇宙是一团能量，把这团能量比作水，去观察一个事物是什么状态的时候，就相当于我们拿着一个容器去盛水，你用的什么容器它就是什么形态，而在此之前它什么形态都可以是。

叠加态是 0 态和 1 态的任意线性叠加，它既可以是 0 态又可以是 1 态，0 态和 1 态各以一定的概率同时存在。通过测量或与其他物体发生相互作用而呈现出 0 态或 1 态，

任何两态的量子系统都可用来实现量子比特，例如，氢原子中的电子的基态和第一激发态、质子自旋在任意方向的+1/2分量和-1/2分量、圆偏振光的左旋和右旋等。

一个量子系统包含若干粒子，这些粒子按照量子力学的规律运动，称此系统处于态空间的某种量子态。这里所说的态空间是指由多个本征态(eigenstate)（即基本的量子态）所组成的矢量空间，基本量子态简称基本态(basic state)或基矢(basic vector)。

态空间可用希尔伯特空间（线性复向量空间）来表述，即希尔伯特空间可以表述量子系统的各种可能的量子态。为了便于表示和运算，Dirac提出用符号$|x\rangle$来表示量子态，$|x\rangle$是一个列向量，称为ket；它的共轭转置(conjugate transpose)用$\langle x|$表示，$\langle x|$是一个行向量，称为bra。一个量子比特的叠加态可用二维希尔伯特空间（即二维复向量空间）的单位向量来描述。

足球赛中的点球能在同一时间既进球得分又错失球门吗？对于非常小的物体，这是可能的。大约100年前，物理学家海森伯创建了一个新的物理学领域——量子力学，根据量子理论，量子世界的物体不再沿着明确的路径移动，取而代之的是，它们可以采用不同的路径同时到达终点，科学家称之为量子叠加态。原子确实看起来遵循量子力学规律运动。

多年过去了，很多实验已经证实了量子力学的预测。但是，在宏观日常生活经验中，足球沿着精确的路线飞行，却从来不会发生同时得分和错失球门的情形。

为什么大的物体不会发生微观物体能产生的叠加态呢？

“有两种不同的解释。”伯恩大学应用物理研究所安德里亚·阿尔贝蒂博士说，“量子力学允许大的宏观物体产生叠加态，但是这种叠加态非常脆弱，即使只用眼睛追随足球就足以破坏叠加态，然后让它按照确定轨迹前进。”但也可能那些足球遵循了完全不同的规则。他说：“宏观现实理论的解释认为，足球总是沿着特定轨迹前进，独立于我们的观察，而且这与原子运动规律完全相反。”

上述两种解释哪种是正确的？大的物体跟小物体运动方式不同吗？

为了验证这一科学猜想，科学家进行了无数验证实验，其中最有名的是下面的一些实验。

3. 铯原子量子叠加态实验

科学家已经间接测量到铯原子量子叠加态，据报道，德国伯恩大学的物理学家设计了一个实验，如图 5-5 所示。首次实验结果就证明铯原子确实在同一时间采取了两条路径。

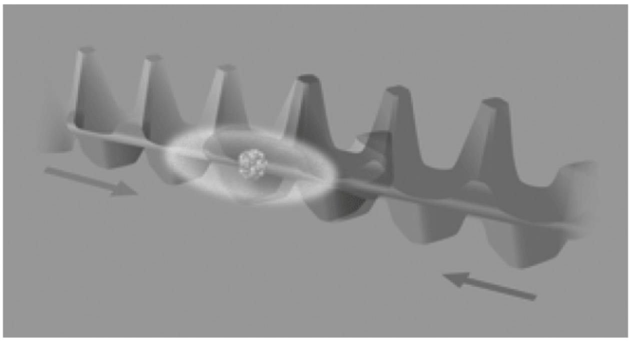


图 5-5　铯原子量子叠加态实验

伯恩大学团队与英国赫尔大学克里夫・埃默里博士合作设计出的一个实验方案或许能解决这个问题。最大的挑战在于制定一个能颠覆宏观现实理论的测量原子位置的方法。

物理学家们在《物理评论 X》上描述了他们的研究成果，他们用两个光学小镊子抓住一个单独的铯原子，并将它向两个方向拉。在宏观现实理论中，这个原子最终会到达其中一个方向。量子力学观点则认为，这个原子能在两个位置上保持稳定性叠加态。

观察结果排除了铯原子遵照宏观现实理论的可能性。相反，伯恩团队的实验结果与叠加态理论解释很契合，研究人员说：“我们现在用最温柔的间接测量方法来确定了原子的最终位置。”但是当非直接的测量发生时，叠加态又被破坏了。现在能做的，就是接受原子确实同时采取了不同路径的事实。

阿尔贝蒂提示说：“现在还不能证明量子力学也适用于大物体。下一步会将铯原子的两个位置分开数毫米，如果在接下来的实验中还找到叠加态，那么宏观现实理论将再次遭受打击。”

4. 双缝干涉实验

双缝实验是著名的光学实验。1807 年，托马斯・杨总结出版了他的《自然哲学讲

义》，里面综合整理了他在光学方面的工作，并在里面第一次描述了双缝实验：把一支蜡烛放在一张开了一个小孔的纸前面，这样就形成了一个点光源（从一个点发出的光源）。现在在纸后面再放一张纸，不同的是第二张纸上开了两道平行的狭缝。从小孔中射出的光穿过两道狭缝投到屏幕上，就会形成一系列明、暗交替的条纹，这就是现在众人皆知的双缝干涉条纹。

在量子力学里，双缝实验是一个测试量子物体像光或电子等的波动性质与粒子性质的实验。双缝实验所需的基本仪器设置很简单。拿光的双缝实验来说，照射相干光束于一块内部刻出两条狭缝的不透明挡板。在挡板的后面，摆设了照相底片或某种侦测屏，用来记录通过狭缝的光波的数据。

从这些数据，可以了解光束的物理性质。光束的波动性质使得通过两条狭缝的光束互相干涉，造成了显示于侦测屏的明亮条纹和黑暗条纹，这就是双缝实验著名的干涉图案。可是，实验者又发觉，光束总是以一颗颗粒子的形式抵达侦测屏。

双缝实验也可以用来检测像电子一类粒子的物理行为，虽然使用的仪器不同，都会得到类似的结果，显示出波粒二象性。

5. 光的波动

在光子的情形下，如果我们取它的波长作为其“尺度”的度量，则第二条缝离开第一条缝大约有300倍“光子尺度”那么远（每一条缝大约有两个波长宽），这样当光子通过一条缝时，它怎么会知道另一条缝是否被打开呢？事实上，对于“对消”或者“加强”现象的发生，两条缝之间的距离在原则上没有受到什么限制。

当光通过缝隙时，它似乎拥有像波动而不像粒子那样的行为。这种抵消和对消干涉现象是波动的一个众所周知的性质。原来两条路径中的每一条分别都可让光通过，而两条同时都开放，则它们完全可能会相互抵消。

这种现象发生的原因：如果从一条缝隙来的一部分光和从另一条缝隙来的“同相”（也就是两个部分波的波峰同时发生，波谷也同时发生），则它们将互相加强。但是如果它们刚好“反相”（也就是一个部分波的波峰重叠到另一部分的波谷上），则它们将互相抵消。

在双缝实验中，只要屏幕上到两缝隙的距离之差为波长的整数倍的地方，则波峰和波

峰分别在一起发生，因而是亮的。如果距离差刚好是这些值的中间，则波峰就重叠到波谷上，该处就是暗的。

关于通常宏观的经典波动同时以这种方式通过两个缝隙没有任何困惑之处。波动毕竟只是某种媒质(场)或者某种包含无数很小点状粒子的物体的一种“扰动”。扰动可以一部分通过一条缝隙，另一部分通过另一条缝隙。

但是这里的情况非常不同，每一个单独光子自身是完整的波动！在某种意义上讲，每个粒子一下通过两条缝隙并且和自身干涉！人们可将光强降得足够低使得保证任一时刻不会有多于一个光子通过缝隙的附近。

对消干涉现象使得两个不同途径的光子互相抵消其实现的可能性，是加在单独光子之上的某种东西。如果两个途径只有一个开放，则光子就通过那个途径。但是如果两个途径都开放，则可能奇迹般地互相抵消，而发现光子不能通过任一条缝隙！

5.2.2 黑道：量子相干性

1.“量子相干性”——量子信息的优势所在

现在各国科学家都在努力希望实现量子计算机，而量子计算机需要一些重要的量子性质。其一是“量子相干性”。

量子相干性也称为态之间的关联性。一种说法是爱因斯坦和其合作者在1935年根据假想实验做出的一个预言。这个假想实验是这样的：在高能加速器中，由能量生成的一个电子和一个正电子朝着相反的方向飞行，在没有人观测时，两者都处于向右和向左自旋的叠加态。进行观测时，如果观测到电子处于向右自旋的状态，那么正电子就一定处于向左自旋的状态。这是因为，正电子和电子本是通过能量无中生有而来，必须遵守能量守恒定律。也就是说，“电子向右自旋”和“正电子向左自旋”的状态是相关联的，称为“量子相干性”。这种相干性只有用量子理论才能说明。

量子相干性来自于量子叠加原理，它是量子力学最基本的特性，也是量子信息的优势所在。对于量子相干性的研究由来已久，从最早的双缝干涉，到量子信息兴起后量子相干性的各种应用及如何克服退相干问题等。

以前测量量子相干性的办法都是利用量子态扫描得到系统整个量子态密度矩阵，再

根据其非对角元的大小间接地得到系统的量子相干性的信息，但是量子态扫描的过程非常烦琐。

近几年，科学家们将量子相干性与量子纠缠等一起纳入资源化理论框架下，确立为量子资源并进行定量研究。量子相干性无疑是其中最宽泛、最基本的量子资源，在某种意义上量子纠缠及其他量子资源都是以量子相干性为基础的。这些工作为我们直接有效地测定物理系统量子相干性的大小打下了理论基础。测度量子相干性的实验光路图如图5-6所示。

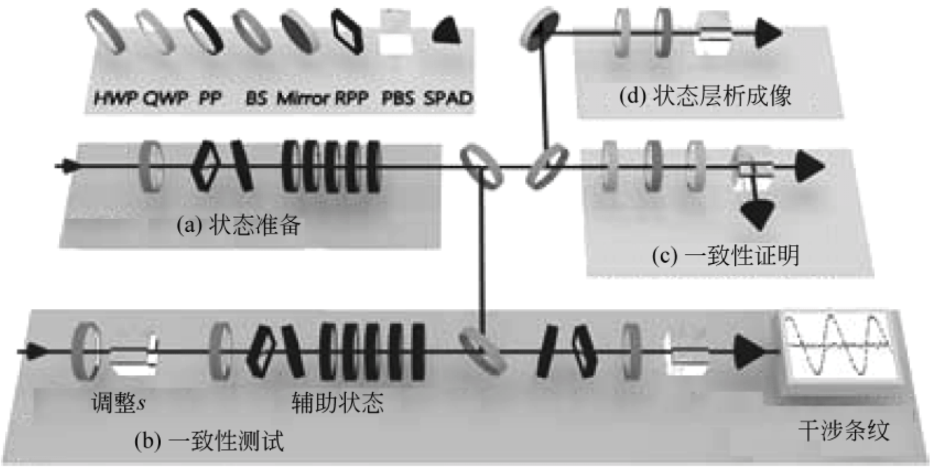

HWP
QWP
PP
BS
Mirror
RPP
PBS
SPAD
(d) 状态层析成像
(a) 状态准备
(c) 一致性证明
调整*s*
辅助状态
(b) 一致性测试
干涉条纹

图5-6　测度量子相干性的实验光路图

要想在量子计算机中实现高效率的并行运算，就要用到量子相干性。彼此有关的量子比特串列，会作为一个整体动作。因此，只要对一个量子比特进行处理，影响就会立即传送到串列中多余的量子比特。这一特点，正是量子计算机能够进行高速运算的关键。

现在各国科学家都在努力希望实现量子计算机，而量子计算机需要一些重要的量子性质，其一便是量子相干性。

2 量子退相干（波函数坍缩）——噪声与干扰

在量子力学里，开放量子系统的量子相干性会因为与外在环境发生量子纠缠而随着时间逐渐丧失，该效应称为量子退相干，又称为量子去相干。

量子退相干是量子系统与环境因量子纠缠而产生的后果。由于量子相干性而产生的

干涉现象会因为量子退相干而变得消失无踪。量子退相干促使系统的量子行为变迁成为经典行为，该过程称为“量子至经典变迁”。德国物理学者汉斯·泽贺最先于1970年提出量子退相干的概念。自1980年以来，量子退相干已成为热门研究论题。

退相干的通俗称谓是“波函数坍缩效应”，是量子力学的基本数学特性之一。夸张地说，退相干效应指的是“当没有人看月亮时，月亮只以一定概率挂在天上；当有人看了一眼后，月亮原来不确定的存在性就在人看的一瞬间突变为现实”。

在实现量子计算机方面，量子退相干是一种必须面对的挑战，因为量子计算机的运作依赖维持量子相干态的演化不被环境搅扰。简言之，必须维持好量子相干态与管控量子退相干，才能够实际进行量子运算。

量子计算机之所以能够完成那些传统计算机所无法企及的复杂计算，在很大程度上都是源于其利用这种独特的量子效应。但量子比特并不是一个孤立的系统，很容易与外部环境发生相互作用，并最终导致量子比特由相干叠加态退化为混合态或单一态，即量子退相干。

虽然量子退相干只是一种噪声或者干扰，但它足以将量子计算机的独特功能破坏殆尽。因此，量子退相干也被看作是量子计算机的一大漏洞。为了克服退相干，科学家尝试过量子纠错码和量子避错码等方法，虽然适用性好，但效率上并不理想。

量子退相干不是一种量子力学诠释，而是利用量子力学分析获得的结果。它严格遵守量子力学，并没有对量子力学的基础表述做任何修改。很多完成的量子实验已证实量子退相干的存在与正确性。

5.3　量子计算独门绝技：量子算法

量子计算的原理实际上应该分为两部分：一部分是量子计算机的物理原理和物理实现；另一部分是量子算法。

量子算法的核心是利用量子计算机的特性加速求解的速度，可以达到经典计算机不可比拟的运算速度和信息处理功能。目前大致有五类优于已知传统算法的量子算法：基

于傅里叶变换的量子算法、以 Grover 为代表的量子搜索算法、模拟量子力学体系性质的量子仿真算法、“相对黑盒”指数加速的量子算法和相位估计量子算法。

量子计算机的运行是对量子比特的操作，从一个量子态演化到另一个量子态，决定两个量子态如何演化的是量子门，其实质是一个遵循量子力学的幺正算符。

以上特质决定了量子计算机的算法与传统算法不同。其一，量子比特是可叠加态（这意味着量子计算机可以进行真正意义上的并行计算），而比特只能取 0 或 1；其二，量子比特的演化必须是幺正的，而比特之间如何变化没有具体约束（一个简单的例子：量子态的演化必须是可逆的，而传统计算机里很多逻辑门都是不可逆的，如与非门）。

Grover 搜索算法和 Shor 质因数分解算法是量子计算中最为经典且重要的两个算法。Shor 算法利用了量子傅里叶变换和一些数论的理论，非常令人震撼，其在破解银行等领域的密钥方面的作用一直被视为量子计算机的重要应用之一。

5.3.1　高等数学+ ：基于 Shor 分解大数质因子量子算法

分解质因数是把合数用几个质数相乘的形式表现出来，一般先用这个合数最小的那个因数（是质数的因数）去除，商如果是合数，就继续除；商如果是质数，就写成商乘除数的形式。

$$30=2\times3\times5$$

$$36=2\times2\times3\times3$$

$$45=3\times3\times5$$

$$50=2\times5\times5$$

例如，把 30 来分解质因数，它最小的因数是（一定用合数除）2，30 除以 2 等于 15，15 是合数，就继续除，15 最小的因数是 3，15 除以 3 等于 5，5 是质数，就不用继续除了。接着把分解出的几个数字写成连乘的形式，即 $30=2\times3\times5$。

分解质因数一般用短除法，如图 5-7 所示。

大数分解说的是一个很大的数能分解成两个素数的乘积。如果这个数非常大，例如它有 100 多位，那么要把它分解目前还没有一个有效算法的。

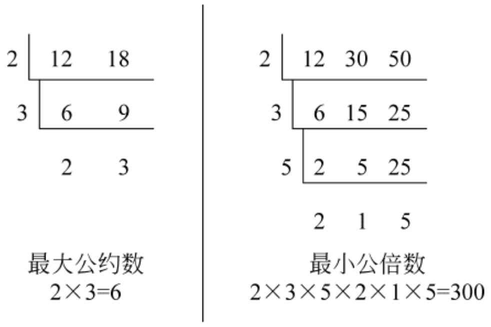


图 5-7　最大公约数与最小公倍数算法

量子分解算法是 1995 年由美国科学家 Shor 提出的，Shor 算法是迄今量子计算领域最著名的算法。它利用量子计算的并行性，可以快速分解出大数的质因子，将使量子计算机很容易破解目前广泛使用的密码（如 RSA 公钥加密系统），严重威胁到银行、网络和电子商务等的信息安全以及国家安全。因此，Shor 算法的提出迅速引起了世界各国对量子计算研究的高度关注。

Shor 算法的基本思想：利用数论相关知识，通过量子并行的特点，获得所有的函数值；再随机选择比自变量小且互质的自然数，得到相关函数的叠加态；最后进行量子傅里叶变换得最后结果。就目前而言，该算法已经相对成熟，对其进行优化的空间不大。Shor 算法及其实现，对量子密码学和量子通信的发展有着极重要的价值。

5.3.2　百度一下：基于 Grover 量子搜索算法

Grover 量子搜索算法通常用于在无序数据库中搜索某一特定的数据。具体来说，该算法适用于解决从 N 个未分类的客体中寻找出某个特定客体的问题。

经典计算对待这类问题一般是逐一进行搜寻，直到找到所需的客体，平均需要寻找 $N/2$ 次才能以 1/2 的概率找到需要的数据。

在量子计算中，Grover 量子搜索算法使用 Oracle 黑箱技术对目标数据进行标识，并利用量子叠加和量子纠缠的特性，使得每一次查询操作可以同时检查所有的数据，这样重复 $\sqrt{N}$（根号下 N）次后，就可平均以 1/2 的概率找到，依此再多重复进行几次操作，便可

以以较高的概率(接近于1)找到那个特定的数据。具体算法如下。

(1) 初始化。应用Oracle算子,检验搜索元素是否是求解的实际问题中需要搜索的解。

(2) 进行Grover迭代。将结果进行阿达马门变换。

(3) 将结果进行运算。

(4) 将结果进行阿达马门变换。

5.3.3　量子智能计算

自Shor算法和Grover算法提出后,越来越多的研究员投身于量子计算方法的计算处理方面,同时智能计算向来是算法研究的热门领域,研究表明,两者的结合可以取得很大突破,即利用量子并行计算可以很好地弥补智能算法中的某些不足。

目前已有的量子智能计算研究主要包括量子人工神经网络、量子进化算法、量子退火算法和量子免疫算法等。其中,量子人工神经网络算法和量子进化算法已经成为目前学术研究领域的热点,并且取得了相当不错的成绩,下面以量子进化算法为例进行介绍。

量子进化算法是进化算法与量子计算理论结合的产物,该算法利用量子比特的叠加性和相干性,用量子比特标记染色体,使得一个染色体可以携带大量的信息。同时通过量子门的旋转角度表示染色体的更新操作,提高计算的全局搜索能力。

目前量子进化算法已经应用于许多领域,例如,工程问题、信息系统、神经网络优化等。同时,伴随着量子算法的理论和应用的进一步发展,量子进化算法等量子智能算法有着更大的发展前景和空间。

5.4　量子计算机的细胞核:门电路

经典计算机的线路由连线与逻辑门组成。连线用于在线路之间传送信息,而逻辑门负责处理信息,将信息从一种形式转换为另一种。

到目前为止,电子计算机与理论中的未来计算机使用的都是冯·诺依曼结构,它们之

间的不同主要是传输与计算的“信号”之间的不同。在传统计算机中，输入的信号是某个量的本征态，简单地说，就是在传统的经典物理学范畴内只能够观测到唯一结果的量，例如一个二进制数字 0110110。当然，经过计算之后，输出的信号也是这样。

电子计算机的运算单元中最基本的部件被称为“门”，是所有逻辑运算的基础。门有多种类型，如与门、或门、非门、与或门、与非门等。举例来说，非门最简单。基于二进制的特性，让你输入 0 时，非门会得到结果 1；输入 1 时，结果则是 0。与门稍微复杂一点，能对同时输入的两个量做出判断。输入 0、0 结果为 0，输入 0、1 结果为 0，输入 1、0 结果为 0，输入 1、1 结果为 1。简单地说，当所有输入都为高值，结果才为高值；只要有一个低值，结果就为低值。

电子计算机的逻辑电路就是用这样无数个门组成。门组成加法器，进而实现更复杂的运算。如同二进制的特点，电子计算机使用的半导体元件有且只有两个状态：开或闭。理论上真正的量子计算机则完全不同。

与经典逻辑门类似，在量子比特上也可以定义逻辑运算，也就是量子比特逻辑门。

由于量子比特对应于量子态，也就是希尔伯特空间的向量，所以量子门会比经典的逻辑门丰富得多。门的操作对应量子态的改变，这可以运用量子运算来描述。17 量子比特芯片如图 5-8 所示。

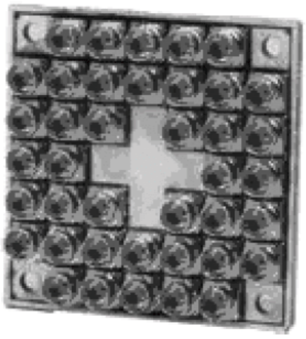


图 5-8　17 量子比特芯片

2018 年 1 月，Intel 公司宣布，Intel 已经成功设计、制造和交付 49 量子比特的超导测试芯片，算力等于 5000 颗 8 代 i7。这距离 Intel 公司 2017 年 10 月交付 17 量子比特芯片仅仅过去了 3 个月的时间。

49 量子比特的芯片代号为 Tangle Lake，被 Intel 公司认为是里程碑。因为在这样的尺度上，已经允许研究人员评估改善误差修正技术和模拟计算问题。谈到量子计算的商用，Intel 公司副总裁兼 Intel 实验室负责人 Mike Mayberry 称，还需要 5～7 年的时间。

7 量子比特、17 量子比特、49 量子比特芯片如图 5-9 所示。

除了超导量子比特，Intel 公司也基于 300nm 制程打造了 1 量子比特的自旋芯片。自

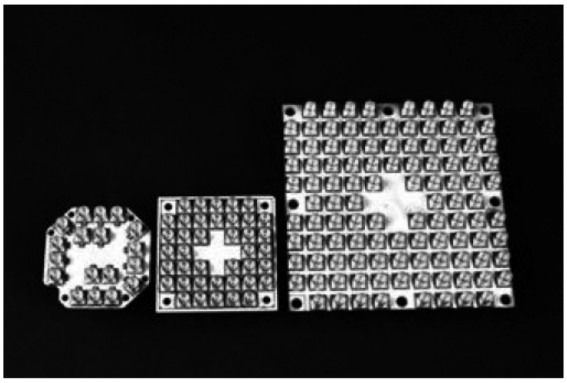


图 5-9　7 量子比特、17 量子比特、49 量子比特芯片

选量子比特的规模和单位面积比超导量子比特更可观，而且，它就像一个单电子晶体管。此前，IBM 公司宣布搞定了 50 量子比特的计算机。

传统计算机都是基于二进制，也就是只能用 0 和 1 来记录所有的信息状态，每一步能做到的只有 2^1 次运算。2 量子比特的量子计算机，每一步可做到 2^2 次运算，所以 Intel 公司的这颗芯片一步就达到 2^{49} 次运算，也就是 562 万亿次。包括 IBM 公司在内，现在正向 50 量子比特迈进，一旦攻克，将超越现存所有的超级计算机。

但我们现在依然需要认识到：量子计算依然是一个相当理论的东西，估计人们需要集成上百万个量子比特的芯片才能真正投入使用，如你所见，Intel 公司刚刚展出的量子超导芯片只有 49 量子比特。据预测，行业已经开始解决如此复杂的芯片工程问题，但这至少需要 5～7 年。

除了超导量子芯片的研究，Intel 公司还在研究一种自旋量子比特芯片，这种芯片的大小比超导芯片体积更小，Intel 公司现在已经开发出了一种能在 300nm 工艺上制造自旋量子比特的方法，这是一种比现在的芯片制造更精细的技术。

所有这些努力，都是为了制造出一个真正的量子计算机。而 Intel 公司也不是唯一一个追求这一目标的公司，IBM 公司就展出了一个巨大的 50 量子比特的量子计算机。

我们非常乐意看到科技巨头之间的技术竞争，这样才能尽快看到下一个时代究竟是什么样子。

5.4.1 华山论剑门派一：量子逻辑门

在量子计算中，特别是量子线路的计算模型里面，一个量子门（Quantum gate，或量子逻辑门）是一个基本的、操作一个小数量量子比特的量子线路。它是量子线路的基础，就像传统逻辑门跟一般数字线路之间的关系。

与多数传统逻辑门不同，量子逻辑门是可逆的。然而，传统的计算可以只使用可逆的门表示。举例来说，可逆的Toffoli门可以实现所有的布尔函数。这个门有一个直接等同的量子门，因此，量子线路可以模拟所有传统线路的操作。

量子逻辑门使用酉矩阵（实正交矩阵）表示。就像常见的逻辑门，一般是针对一个或两个比特进行操作，常见的量子门也是针对一个或两个量子比特进行操作。这也代表着一些量子门可以用2×2或者4×4的酉矩阵表示。

1. 量子逻辑

在现代信息理论与技术中，逻辑电路是实现整个理论及技术的关键，其中，最基本的逻辑单元有三个：与门、或门、非门。由这些基本的逻辑门组成经典通用逻辑门组，实现各种逻辑功能的变换与处理。

由于经典逻辑门的实现是半导体材料，即通过半导体材料中大量电子运动的宏观统计来表征其逻辑关系，这种电子运动的宏观统计服从于经典物理学所规定的规律。如果将半导体材料中的电子数减少到一个或少数几个，即减小半导体元件的尺寸到电子的数量级时，则电子的行为不再遵循经典物理学的规律，而是服从量子物理学所规定的定律和方法，此时，再用经典的方法描述逻辑门，其逻辑关系将变得模糊。因此，在理论上将其逻辑电路区分为经典逻辑和量子逻辑。

量子逻辑就是利用微观粒子的量子态（行为），通过一系列幺正操作，实现量子态的变换以及进行各种逻辑关系的运算。量子逻辑与经典逻辑最本质的区别主要表现在以下几个方面。

（1）经典逻辑的理论满足于经典物理学所规定的定律、方法和技术；量子逻辑的理论则遵循量子物理学所规定的定律、表述方法。前者表现为宏观统计性质上的物理描述；后

者表现为微观粒子个体以及微观粒子个体之间相互作用的物理描述，是前者理论和技术的进一步拓展和延伸。

(2) 经典逻辑关系是对信息量(比特)进行一系列的布尔变换；量子逻辑则是对量子信息的量(量子比特)进行一系列的幺正变换。

(3) 在现有的经典逻辑电路中，其变换关系是不可逆的，虽然有人曾试图理论证明，经典逻辑门在一定的条件下可以转变成可逆。但由于其系统的热运动不可避免，存在能量损耗。因此，其操作是不可逆的。

在量子逻辑电路中，由于其描述方法及理论是量子态的行为，体现为操作上的幺正变换。因此，对态的操作应是幺正的、可逆的，无能量损耗。

(4) 经典逻辑电路的实现是在相空间中进行，而量子逻辑电路的实现则是在希尔伯特空间中进行，是复矢空间。

(5) 经典逻辑所表现的是两个比特之中的一个，即两个状态中的真或假，0 或 1。量子逻辑所表现的是两个量子比特之间的不同线性叠加的结果，既可以是 0 或 1，也可以是 0+1，0-1，还可以是 0 和 1 之间的任一形式。因此，无论是从理论上还是技术上，量子逻辑是经典逻辑无法比拟的，它是经典逻辑的进一步拓展和延伸。

(6) 经典逻辑门可以有多个输入，但它却只有一个输出。量子逻辑门有多个输入，同时存在着多路输出。

2 量子逻辑门

在经典逻辑电路中，门电路是逻辑电路的最基本单元，它是利用半导体材料中电子的宏观运动所表现的特性来表征。

量子逻辑门同样是量子逻辑电路的最基本单元，只不过它已不再是用电子的宏观统计特性来表征，而是用微观粒子的个体行为状态来描述，它将一个态演化为另一个态。例如，电子等微观粒子的自旋、电子在不同能级上的跃迁等。理论和实践技术证明，由最基本的量子逻辑门所组成的通用逻辑门以及逻辑关系是经典通用逻辑门和逻辑关系不可比拟的。

量子逻辑电路中，最基本的逻辑门有与门、非门和复制门，以此为基础构成一位量子

逻辑门、二位量子逻辑门和三位量子逻辑门。在经典信息理论中，信息量的基本单位为比特，一个比特是给出经典二值系统一个取值的信息量。在量子信息理论中，量子信息的基本单位是量子比特。一个量子比特是一个双态量子系统，即一个量子比特就是一个二维希尔伯特空间。量子逻辑门的本质是对量子比特实施最基本的幺正操作。

与经典逻辑最基本的与门、非门、或门有其本质的区别，量子逻辑门除具有经典逻辑门的所有特征外，还具有改变量子态的相对位相的门、Hadamard 旋转门和一个恒等操作门，即作用到两个量子比特上的所有可能的幺正操作构成二位量子逻辑门。由一位、二位和三位量子逻辑门构成量子通用逻辑门组。

1995 年，Deutsch 证明，几乎任意的二位量子门或 n 位量子门对量子计算构成实际的通用逻辑门组。同时，Barenco 等人又证明，通用量子门还可由经典多位门和量子一位门构成。

3.量子逻辑门的物理实现及进展

由于最基本的逻辑门是受控的两量子比特的物理系统，在两量子比特系统之间根据一个比特的状态条件对另一个比特实现所需要的幺正演化、控制两量子比特之间的转动就足以构造出能执行任意复杂的量子计算网络。因此，量子逻辑门的实现是量子计算的关键。

目前，构造量子逻辑门的实验方案主要有以下几种。

1）离子阱方案

量子逻辑门的最初离子阱方案由 Cirac 提出。它是在特定构形的电极上加上静电场、交变电场或磁场的适当组合，将带电离子稳定地囚禁于高真空的一种装置。利用这种装置将离子冷却至质心运动状态的基态，从而使离子处于用来表征量子信息的量子比特上，并通过辅以特定的操作，实现量子逻辑门。该方案由于与外界的相互作用极弱，因此，由环境所引起的消相干效应可忽略不计；另外，由于处于阱中的 n 个超冷离子是排成一行的，所以，可实现 n 位的量子逻辑门。连接 n 位量子逻辑门的“导线”就是 n 个超冷离子在阱中的集体振荡。

由于离子冷却的难度很大，所以很难推广至多个超冷离子的制备。与此同时，人们不

断地提出其他的可能实现方案，1998年，Poyatos提出不用超冷离子也能实现量子逻辑门的方案，即“热”离子方案。其基本思想是在对量子比特的操作中只依赖于离子的内态，而与外态无关，即无论外界处于何种状态，离子都能进行任意的量子操作。2000年，Cirac和Zoller提出一种新的基于椭圆形离子阱构形的方案，该方案避免了多个离子之间的库仑排斥的影响，易于集成。但真正实现该方案，在技术上仍存在很大的难度。

2）腔量子电动力学方案

在单原子、单光子水平实验的技术基础上，1995年，Barenco和Sleator等人同时提出实现两量子比特控制转动操作的腔QED方案。在该方案中，量子比特由高Q微波腔内的量子化电磁场和两能级原子充当。当原子通过腔场时原子和腔场作用的时间，决定了腔场的态及原子的运动速度，从而实现了所需要的条件量子相移门和控制非门。

之后，Giovannetti等证明，腔与原子体系不仅可以实现控制非门、条件量子相移门、单量子比特的任意操作，而且还可以实现Toffoli门、Deutsch门和进行量子纠错编码，使腔与原子体系进行多位量子逻辑计算真正成为现实。2000年以后，新一代的腔量子电动力学实验取得了突破性进展。应用这些新的技术，有望在不久的将来，实现更多的量子信息的处理器件和建立未来的光量子网络。

3）固态量子体系方案

1999年，Nakamura等人利用超导约瑟夫森结第一次实现了固态量子逻辑门。在实验中，超导约瑟夫森结起两个重要作用。

（1）实现单个库珀对在其中的隧道过程。

（2）使能级出现免交叉效应。能在宏观的超导箱中实现一个二能级的量子体系。随后，Makhlin等首先讨论了单个库珀对的量子逻辑操作。2001年，赵志等人证明，使用超导量子干涉，也可实现量子逻辑操作。

在固态量子体系方案中，另一个可能实现量子逻辑门的体系是量子点。量子点是把半导体材料中几百个原子组成纳米尺度的小岛，或把半导体材料中的单电子视为量子点，将它们所处的基态和激发态看作一个二能级量子体系，操纵量子点状态之间的变化，即可实现量子逻辑门。

4）核磁共振方案

核磁共振技术是目前量子信息技术使用最为频繁的实验手段，已提出的各种量子算法都能在几个量子比特下进行验证。在这一技术中，操作并非作用在某个单独的粒子或分子的自旋上，而是作用在10^{23}数量级的系综的自旋态上。因此，它实质上是一个宏观系综。由于它是宏观系综，因此，几乎不受外部环境对它的影响。但宏观系综原则上是没有量子特性的，只有纯粹的量子系综才具有量子纯态的特征，因而对它存在较大争议。

从目前所提出的所有实现量子逻辑门方案及实验来看，固态量子体系的实验进展不如离子阱和腔量子电动力学的实验进展，从各方面的研究报告统计可以证实。由于固态量子体系方案，特别是量子点方案能镶嵌在固体材料中，所以，吸引了一大批理论和实验学家，并利用半导体纳米技术，使得在不久的将来量子点方案的实现成为最可能实现的方案。

5.4.2 华山论剑门派二：单量子比特门

1. 单量子比特的里德伯门

目前，物理学家已经成功构建了单量子比特的里德伯门，激光将一个锶离子激发到里德伯激发态，如图 5-10 所示。这一技术是打造里德伯离子阱量子计算机的基本要素之一。这一成就说明了制造新型量子计算机的可行性，并有望克服当前量子计算方法面临的量子数量增加时遇到的难题，新型量子计算机近在咫尺。

目前，量子计算机面临的最大挑战之一是如何按比例增加每个逻辑门中的纠缠量子比特数量，这对于进行实际的量子计算至关重要。在某种程度上，增加数量如此困难的部分原因是，离子阱系统中常用的多比特量子门随着量子比特数量的增加会产生频谱拥挤的问题。然而，里德伯离子阱系统能有效避免频谱拥挤的干扰，这就意味着如果用里德伯离子阱量子比特来制造量子计算机，就可能为量子计算机在量子数量增加时遇到的瓶颈问题提供了新的解决路径。

在目前的研究中，研究人员建造了第一个单量子比特的里德伯门，他们预计能够将单量子位的版本升级成一个双量子比特的里德伯门，并在将来增加更多的量子数量。

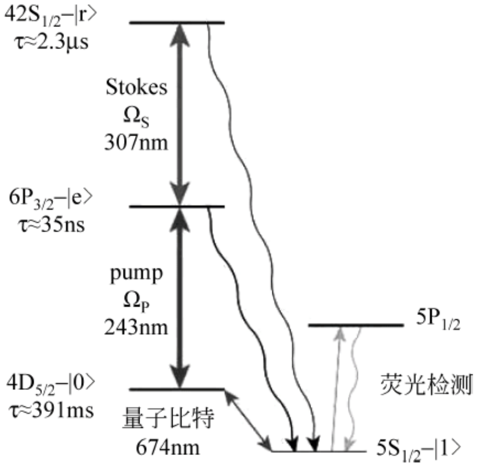

$42S_{1/2}$–|r〉
τ≈2.3μs
Stokes
Ω_S
307nm
$6P_{3/2}$–|e〉
τ≈35ns
pump
Ω_P
243nm
$5P_{1/2}$
荧光检测
$4D_{5/2}$–|0〉
τ≈391ms
量子比特
674nm
$5S_{1/2}$–|1〉

图 5-10　激光将一个锶离子激发到里德伯激发态

2. 新型量子计算机首个基本元件问世

单量子比特的里德伯门扩展性更强、运算速度更快，瑞典和奥地利物理学家携手，研制出了单量子比特的里德伯门，这是囚禁的里德伯离子量子计算机的首个基本元件。最新研究证明了建造这种量子计算机的可行性，其有潜力克服目前的量子计算方法面临的扩展问题。

实验的关键之处在于，里德伯态采用相干方式获得，这对于建造多量子比特里德伯门至关重要。研究人员将相干的里德伯激发与量子操控方法相结合，展示了单量子比特里德伯门。他们估计，可将这一单量子比特系统扩展到二量子比特系统，未来还可以添加更多量子比特。

除了潜在的升级优势，基于囚禁的里德伯离子而研制的量子计算机还拥有其他优势，包括能更好地控制量子比特、门运算速度更快等，他们将进一步研究这些可能性。

5.4.3　华山论剑门派三：条件非门

量子技术重大突破：由硅制成的量子可控非门

比起实现量子计算机的其他现有技术，硅基设备很可能是廉价而且容易制造的。尽管其他研究小组和公司已经宣布制造出具有 50 甚至更多量子比特的量子计算设备，但是

这些系统需要超常的材料，例如，超导体或者通过激光照射处于适当位置的带电原子。

美国普林斯顿大学科研人员领导的团队，如图 5-11 所示，在采用日常材料制造量子计算机的方面取得重要进展。他们制造出由硅制成的关键硬件，以极高的精准度控制两个电子之间的量子行为。

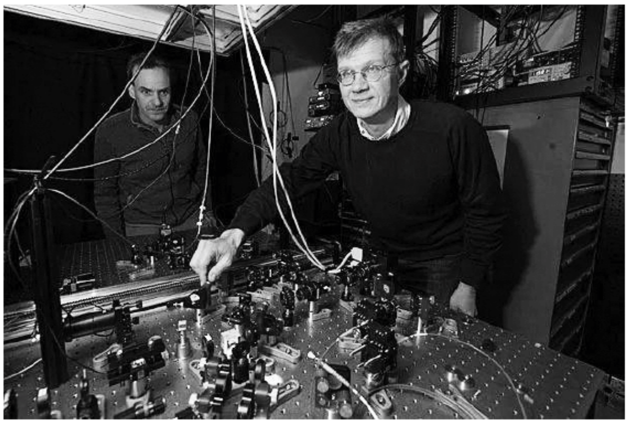


图 5-11　美国普林斯顿大学科研团队

该团队通过一种让电子作为量子信息比特的方式，构建出一种门控制电子之间的交互。这对于量子计算来说很有必要。这种几乎无错的、两个量子比特的门，是通过硅材料构建出更加复杂的量子计算设备方面的早期重要进展，目前硅材料已广泛应用于传统的计算机和智能手机。

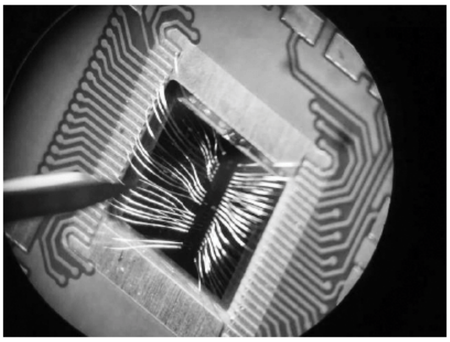


图 5-12　由硅材料制成的关键硬件

研究人员为了构造两个量子比特的门，在高度有序的硅晶体上，分层放置微小的铝线。这些线提供可以囚禁两个单独电子的电压，而电子则通过能阈隔开，形成像井一样的结构，称为双量子点。由硅材料制成的关键硬件如图 5-12 所示。

其挑战在于构建小到足够囚禁和控制单个电子的结构，而又不会破坏它们漫长的存储时

间。这项研究首次展示了硅中两个电子自旋之间的纠缠，硅是一种为电子自旋状态提供最干净的一种环境的材料。研究人员演示他们能够采用第一个量子比特控制第二个量子比特，这意味着该结构可作为一种可控非门（CNOT），如图 5-13 所示，它是普通使用的计算机电子器件的量子版本。

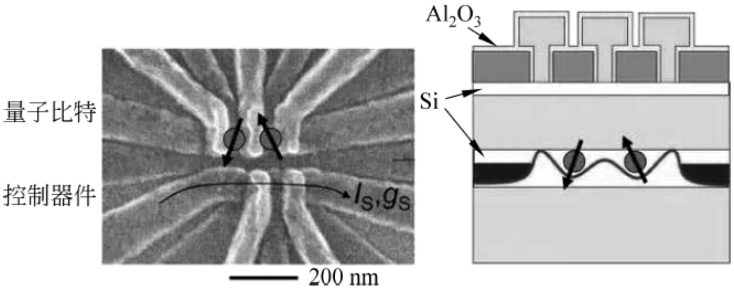


图 5-13　可控非门

研究人员通过施加磁场，控制第一个量子比特的行为。这个门制造出基于第一个量子比特状态的结果：如果第一个自旋指向上方，第二量子比特的自旋将快速翻转；但是如果第一个自旋指向下方，第二个量子比特将不会翻转。

5.4.4　华山论剑门派四：量子芯片

量子芯片就是将量子线路集成在基片上，进而承载量子信息处理的功能。借鉴传统计算机的发展历程，量子计算机的研究在克服瓶颈技术之后，要想实现商品化和产业升级，需要走集成化的道路。

目前，超导系统、半导体量子点系统、微纳光子学系统，甚至原子和离子系统，都想走芯片化的道路。从目前的发展看，超导量子芯片系统从技术上走在了其他物理系统的前面；传统的半导体量子点系统也是目前人们努力探索的目标，因为毕竟传统的半导体工业发展已经很成熟，如半导体量子芯片在退相干时间和操控精度上一旦突破容错量子计算的阈值，有望集成传统半导体工业的现有成果，大大节省开发成本。

中国科学院量子信息重点实验室与合作者成功实现了半导体量子点体系的两个电荷

量子比特的控制非逻辑门，成果于 2015 年 7 月 17 日发表。

一个单量子比特逻辑门操控和一个两量子比特受控非门可以组合任意一个普适量子逻辑门操控，而实现普适量子逻辑门操控是实现量子信息处理过程的最关键技术。

单比特和两比特量子逻辑门的完成，表明量子计算所需的所有基本量子逻辑门都可以在半导体上通过全电控制方式实现。这种方式具有操控方便、速度超快、可集成化并兼容传统半导体电子技术等重要优点，是进一步研制实用化半导体量子计算的坚实基础。

量子芯片是未来量子计算机的“大脑”，量子计算机能够使用亚原子粒子编码数据。专家认为，量子比特同时具有两种状态，能够显著提高计算速度和能力。目前，Google 公司与科学家联手研制量子级计算机处理器，有望未来使机器人像人类一样独立思考问题。

5.4.5 华山论剑门派五：量子传感器

氮原子大小的量子传感器已经研制成功，量子技术为计算机小型化开辟了新途径。德国弗劳恩霍夫应用固体物理研究所的研究人员开发出了一种微磁场下应用的量子传感器，可应用于未来计算机硬盘识别。

集成电路变得越来越复杂。最新的奔腾处理器可容纳约 3000 万个晶体管。硬盘驱动器中的磁性结构，可识别的范围仅为 10～20nm，比直径 80～120nm 的流感病毒还小。

专家通过光学检测电子自旋共振谱测量后表示，这种氮原子传感器检测纳米级磁场的准确性很高，具有惊人的应用潜力。例如，它可以作为量子传感器来控制硬盘驱动器的质量，检测海量数据中有缺陷的数据段。这种量子传感器还可以测量脑电波。

这种量子传感器能非常精准地测量在下一代硬盘中看到的微小磁场。同样，它对磁场的感知也可以避免使用电极测量脑电波时产生的不精确后果。这项神奇的工具还能赋予人们前所未见的新物质状态和物质相，甚至在军事上，成熟的量子传感技术也将带来诸多益处。

5.5　最火的量子计算机来了

量子计算将有可能使计算机的计算能力大大超过今天的计算机，但仍然存在很多障碍。大规模量子计算所存在重要的问题是，如何长时间地保持足够多的量子比特的量子相干性，同时又能够在这个时间段之内做出足够多的具有超高精度的量子逻辑操作。

5.5.1　众说纷纭的理论及研究

1. 世界上第一台商用量子计算机已经出售

加拿大量子计算公司D-Wave早在2011年就正式发布了全球第一款商用型量子计算机——D-Wave One。D-Wave One采用了128量子比特的处理器，理论运算速度已经远远超越现有任何超级电子计算机。不过，严格来说这还算不上真正意义上的通用量子计算机，只是能用一些量子力学方法解决特殊问题的机器。通用任务方面还远不是传统硅处理器的对手，而且编程方面也需要重新学习。另外，为尽可能降低量子比特的能级，需要利用低温超导状态下的铌产生量子比特，D-Wave One的工作温度需保持在绝对零度附近。

2017年1月，D-Wave公司推出D-Wave 2000Q，它们声称该系统由2000量子比特构成，可以用于求解最优化、网络安全、机器学习和采样等问题。对于一些基准问题测试，如最优化问题和基于机器学习的采样问题，D-Wave 2000Q胜过当前高度专业化的算法1000～10000倍。

D-Wave One量子计算机与D-Wave公司创始人兼CTO Geordie Rose如图5-14所示。

尽管在量子性等方面存在争议，但D-Wave公司仍于2011年和2013年卖给美国洛克希德－马丁公司和Google公司各一台，其中卖给Google公司的量子计算机速度据称比普通计算机快3.55万倍。

大多数从事基础量子计算研究的实验室，所研究的系统涉及的量子比特数目仅为个位数，而D-Wave量子计算机的比特数目达到512，已经初步具有解决实际问题的规模。

图 5-14　D-Wave One 量子计算机与 D-Wave 公司创始人兼 CTO Geordie Rose

所以，对其计算速度的研究，特别是与传统计算机在速度上的比较就成为急需解决的一个问题。

这项研究的重要意义就在于给出了“一个合理评估的标准程序”，主要内容是量子计算机能否带来整体计算速度的提高，即“量子加速”。具体来说，他们测量了问题难度提升时 D-Wave 量子计算机与传统计算机所分别增加的计算时间，如果存在量子加速，那么量子计算机增加的计算时间应该比传统计算机少得多。

2. 经典计算机和量子计算机的区别

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。当某个装置处理和计算的是量子信息，运行的是量子算法时，它就是量子计算机。

1）经典计算机

要说清楚量子计算，首先看经典计算机。经典计算机从物理上可以被描述为对输入信号序列按一定算法进行变换的机器，其算法由计算机的内部逻辑电路来实现。

（1）其输入态和输出态都是经典信号，用量子力学的语言来描述，即其输入态和输出态都是某一力学量的本征态。例如，输入二进制序列 0110110，用量子记号，即$|0110110\rangle$。

所有的输入态均相互正交。对经典计算机不可能输入如下叠加态：C1|0110110〉＋ C2|1001001〉。

（2）经典计算机内部的每一步变换都演化为正交态，而一般的量子变换没有这个性质。因此，经典计算机中的变换（或计算）只对应一类特殊集。

2）量子计算机

量子计算机的输入用一个具有有限能级的量子系统来描述，如二能级系统（称为量子比特），量子计算机的变换（即量子计算）包括所有可能的幺正变换。

（1）量子计算机的输入态和输出态为一般的叠加态，其相互之间通常不正交。

（2）量子计算机中的变换为所有可能的幺正变换。得出输出态之后，量子计算机对输出态进行一定的测量，给出计算结果。

由此可见，量子计算对经典计算做了极大的扩充，经典计算是一类特殊的量子计算。量子计算最本质的特征是量子叠加性和量子相干性。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些经典计算同时完成，量子并行计算。

3. 量子计算理论和技术的发展历程

了解了量子计算机领域激烈的巨头混战，那么量子计算理论的发展又是怎么样的呢？

量子计算理论从首次提出到现在已经有 30 多年，在 1981 年时，诺贝尔奖获得者费曼首次提出量子计算机的概念。

1994 年，贝尔实验室的专家 Shor（见图 5-15）证明量子计算机能完成对数运算，而且速度远胜传统计算机，这也是在量子计算理论提出十多年后的第一次实验。

SCATTERED
WAVE K(1,2)
SPACE
1st ORDER
ORDE

图 5-15　贝尔实验室的专家 Shor

自此，投资者开始发现量子计算机的可行性，也许量子计算机未必会有那么多运算错误，也许可以尝试造出一台处于稳定状态的量子计算机。

随后的十几年，无数的资金进入量子计算研究领域，量子计算迎来了很多技术研究进展：D-Wave 的量子退火、Intel 公司的硅量子点等，这些研究成果都各有

优缺点，但是都还没有解决最根本的问题。现在主要的技术难点在于精确地实现量子比特的调控、两两之间的纠缠、维持它们的量子状态等，也就是系统的可控性和可靠性。

技术上的瓶颈并没有得到很好地突破，但是科技巨头们依然在量子计算这条路上你追我赶，为什么呢？主要原因在于现有的芯片线程越来越小（纳米级），量子力学现象会成为计算机的缺陷，这个缺陷具体来说是这样的，计算机里面有很多晶体管，晶体管像一个开关控制电子进程，但是未来的元件做到纳米级后，比如纳米级的晶体管，这个开关可能会失效，因为根据量子力学，电子可以直接通过纳米级晶体管，到了那时，这就会是经典计算机无法解决的大缺陷。

另一方面，因为经典计算机已经快要达到它的极限，其芯片越来越小，芯片的元件小到只有原子大小，而且就算达到极限，经典计算机也解决不了未来可能会出现的许多问题。例如，优化问题，也就是从无数种可能性中找出最优的解决方法，经典计算机只能一个一个地去找，但是量子计算机可以并行运算，毫不夸张地说，经典计算机可能要算一年，量子计算机只用一分钟就能搞定。

还有就是经典计算机在化学问题、生物问题上的无力。研究人员曾经举过一个生动的例子，一个咖啡因分子，如图 5-16 所示，不如水分子简单，但也没有 DNA 或是蛋白质分子复杂，如果用经典计算机来模拟一个咖啡因分子，世界上现有的任何计算机都不行，就算你做再多晶体管，做一个和地球一样大的计算机，或者一个和太阳系一样大的计算机，甚至是和银河系一样的计算机，都没办法模拟一个咖啡因分子，然而量子计算机却可以做到。

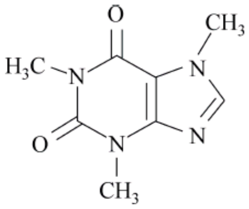


图 5-16　咖啡因分子

总而言之，在经典计算架构发展瓶颈日益突出的当下，量子计算机被认为是计算领域最有发展前途的方向之一。

不过这个未来什么时候才能来，谁都不清楚，也许十年以内不会到来，根据 Intel 公司专家的说法：“我们预计这个行业将需要 5～7 年的时间才能解决工程规模问题，并且可能需要 100 万或更多的量子比特才能达到商业目的。研究人员仍然需要弄清楚如何解决一些问题，包括纠正单个量子比特的脆弱量子态，将软件算法映射到量子硬件，建立局部

控制电子学来控制量子系统并得到结果”。

4. 量子计算机将重造整个世界

量子计算之所以如此重要，除了因为它快，还因为它可以重新定义程序和算法，颠覆众多领域。例如，军事方面，一切现有的密码学全都要被重新改写，因为用量子计算机能轻易地破译所有密码；医学方面，量子计算机可以模拟人体内的各种化学分子，建立起医学模拟的新模型；此外还有气象学、材料科学等领域都面临着量子计算的颠覆。

不过，目前人们离真正的量子计算机还有距离，现在，量子计算机还只是非常初步的阶段，量子比特的脆弱、不稳定性，还有低精度的问题还没有解决，要实现实用量子计算机还有很长的路要走。

5.5.2　信息化战争：量子计算的意义不亚于核武器

倘若人们要追溯风靡全球的信息化战争的科技源头，无疑是1946年世界第一台计算机ENIAC诞生所开启的电子信息科技革命，以及其给战争形态带来的质变——从机械化战争转向信息化战争。然而，这一曾颠覆机械化战争图景的电子信息科技，在遵循“摩尔定律”飞速前行了数十年之后，制约其进一步发展的问题也日渐凸显：电子计算机的极限运算速度是否存在？

从理论上讲，一个250量子比特（由250个原子构成）的存储器，可能存储的数达2^{250}，比现有已知的宇宙中全部原子数目还要多。无论在基础理论还是在具体算法上，量子计算都是超越性的。例如，科学家提出的量子搜寻算法，其计算速度是目前最快的计算机的亿万倍。如果用量子搜寻算法攻击现有密码体系，经典计算需要1000年的运算量，量子计算机只需小于4min。

以致有科学家宣称：“量子计算的意义不亚于核武器……一旦有些国家拥有了量子计算机，而另一些国家却没有，当战争爆发时，这就犹如一个瞎子和一个睁眼的人在打架一样，对方可以把你的东西看得清清楚楚，而你却什么都看不到。”

因此，对量子计算的相关研究及量子计算机的具体研制已成为世界科学领域最闪亮的“明珠”之一。例如，美国国防部对此就给予了高度重视，国防部高级研究计划署专门制

订了名为“量子信息科学和技术发展规划”的研究计划，其对外公开宣称的目标是，若干年内要在核磁共振量子计算、中性原子量子计算、谐振量子电子动态计算、光量子计算及固态量子计算等领域取得重大研究进展。

未来一体化联合作战的关键在于各战场空间、参战军兵种能否联通，实现信息的及时共享。目前，由于网络宽带、通信容道等限制，还难以真正实现信息实时共享。然而，量子通信技术的发展，有可能会使一切难题迎刃而解。航天力量支援下的一体化联合作战示意图如图5-17所示。

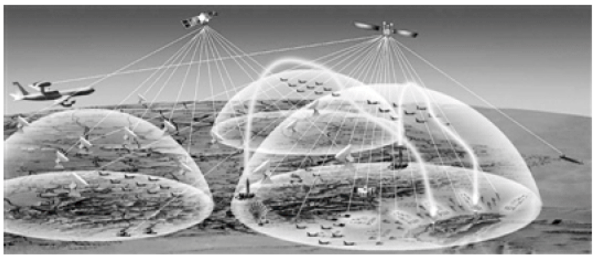


图5-17　航天力量支援下的一体化联合作战示意图

与传统的通信技术相比，量子通信技术具有如下优点。

(1) 安全保密。据有关专家介绍，用光量子电话网，虽然跟平常打电话一样，却不用担心被窃听，相互之间通话绝对安全。这是因为，量子通信采用的是一次一密的加密方式，两人通话期间，密码机每分每秒都在产生密码，牢牢“锁”住语音信息；一旦通话结束，这串密码就会立即失效，下一次通话绝对不会重复使用，而且量子通信所提供的密钥无法被破解。

(2) 超光速传输。与传统光速通信相比，量子超光速通信具有许多人们梦寐以求的优点：量子超光速通信的线路时延可以为零，从而实现了最快通信；量子信息传递的过程不会为任何障碍所阻隔；量子超光速通信完全环保，不存在任何电磁辐射污染。因此，可以利用量子隐态传输以及超大信道容量、超高通信速率和信息高效率等特点，建立满足军事特殊需求的超光速军事信息网络。但目前量子通信仍然必须借助经典光纤信道传输，超光速传输级需要进行大量的理论和实践研究。

(3) 通信距离远。有科学实验证实，量子隐态传输能够穿越大气层，可进行星际联

络。我国科学家近期就在国际上首次成功实现数百千米量级的自由空间量子隐形传态和纠缠分发，并已发射全球首颗“量子通信卫星”。

（4）与传播媒质无关。与现代通信手段不同，量子通信的光量子隐态传输与传播媒质无关，不会因其受阻，因此能够应用于深海安全通信。当前，岸基与深海之间的通信一直是世界性难题。利用长波通信，不仅系统庞大、造价高、抗毁性差，而且仅能实现海水下百米左右的通信。量子通信的这一特性，将为远洋深海安全通信开辟了一条崭新的途径。

由此可见，量子通信技术在军事应用方面有无与伦比的广阔前景。量子隐形通信系统将建立在各类作战指挥控制体系之间和各种侦察预警系统、主要作战平台以及空间武器系统之中，从而构建出量子信息化战场的通信网络，以其超大信道容量、超高通信速率等特性，在未来的信息化战争中扮演无可替代的角色。

5.5.3　分久必合：量子计算机的工作原理

1.“杞人忧天”的物理学家们与量子计算机的诞生

量子计算机的诞生和著名的摩尔定律有关，还和“杞人忧天”的物理学家们有关。

1965年，Intel公司的创始人之一戈登·摩尔，如图5-18所示，针对电子计算机技术的发展提出了“每18个月计算能力翻倍”的摩尔定律。然而，由于传统技术的物理局限性，这一能力或将在未来10～20年之内达到极限。

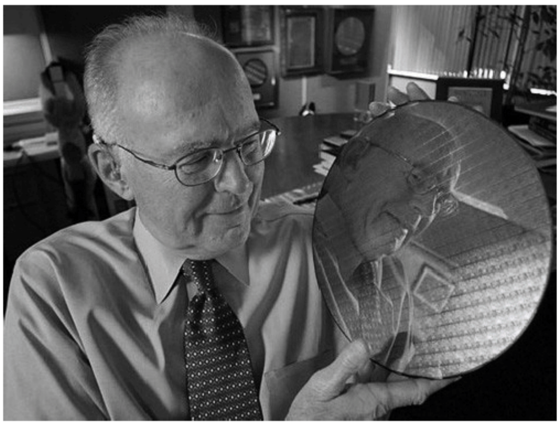


图5-18　戈登·摩尔提出了摩尔定律

众所周知，摩尔定律的技术基础是不断提高电子芯片的集成度（单位芯片的晶体管数）。集成度不断提高，速度就不断加快，我们的手机、计算机就能不断更新换代。摩尔定律的发展曲线如图 5-19 所示。

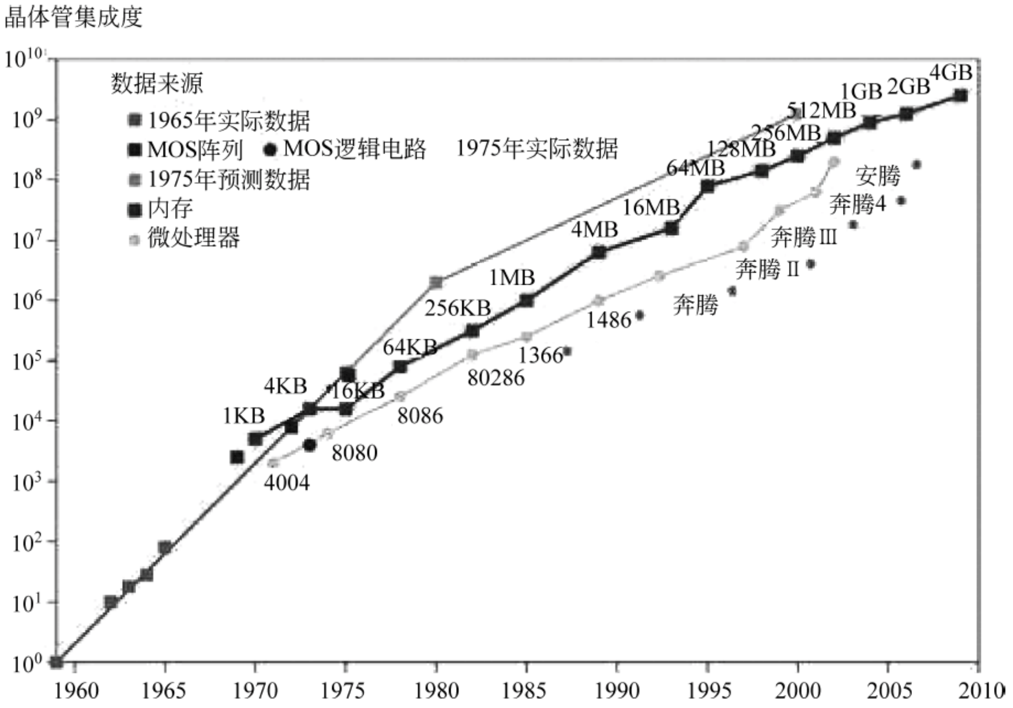


图 5-19　摩尔定律

据保守估计，2018 年芯片制造业就将步入 16nm 的工艺流程，业内专家则认为，16nm 制程已经是普通硅芯片的尽头。事实上，当芯片的制程小于 20nm 之后，量子效应就将严重影响芯片的设计和生产，单纯通过减小制程将无法继续遵循摩尔定律，而突破的希望恰在于量子计算。

在 20 世纪 80 年代，摩尔定律很贴切地反映了信息技术行业发展。但杞人忧天的物理学家们，却提出了一个问题：摩尔定律有没有终结的时候？

之所以提出这个问题，是因为摩尔定律的技术基础，天然地受到两个主要物理限制。

一是巨大的能耗，芯片有被烧坏的危险。

芯片发热主要是因为计算机门操作时，其中不可逆门操作会丢失比特。物理学家计

算出每丢失一个比特所产生的热量，操作速度越快，单位时间内产生的热量就越多，计算机温度必然迅速上升，必须消耗大量能量来散热，否则芯片将被烧坏。

二是为了提高集成度，晶体管越做越小，当小到只有一个电子时，量子效应就会出现。电子将不再受欧姆定律管辖，由于它有隧穿效应，本来无法穿过的壁垒也穿过去了，所以，量子效应会阻碍信息技术继续按照摩尔定律发展。

这两个限制就是物理学家们预言摩尔定律会终结的理由所在。

隧穿效应就是由微观粒子波动性所确定的量子效应，又称为势垒贯穿。本质上是量子跃迁，粒子迅速穿越势垒。在势垒一边平动的粒子，当动能小于势垒高度时，按照经典力学，粒子是不可能越过势垒的；而对于微观粒子，量子力学却证明它仍有一定的概率贯穿势垒，实际也正是如此，这种现象称为隧穿效应。

虽然这个预言在当时没有任何影响力，但杞人忧天的物理学家们并不死心，继续研究，并提出了第二个问题：如果摩尔定律终结，在后摩尔时代，提高运算速度的途径是什么？

这就导致了量子计算概念的诞生。

量子计算所遵从的薛定谔方程是可逆的，不会出现非可逆操作，所以耗能很小；而量子效应正是提高量子计算并行运算能力的物理基础。

甲之砒霜，乙之蜜糖。对于电子计算机来说是障碍的量子效应，对于量子计算机来说，反而成为了资源。

量子计算的概念最早是1982年由美国物理学家费曼提出的。1985年，英国物理学家又提出了量子图灵机的概念，之后许多物理学家将量子图灵机等效为量子的电子线路模型，并开始付诸实践。

但当年这些概念的提出都没有动摇摩尔定律在信息技术领域的地位，因为在相当长时间内，摩尔定律依然在支撑着电子计算机的运算速度的飞速提高。

直到如今，摩尔定律铁定要终结了，微电子未来的发展方向是低能耗、专用这两个方向，而不再是追求速度。

从这个例子，人们再次看到，基础研究可能在当时看不到有什么实际价值，但未来却

会发挥出巨大作用。

2. 量子计算机虽然好，研制起来却非常难

量子计算机和电子计算机一样，其功用在于计算具体数学问题。

其核心操作使用的是幺正变换，即相当于是坐标变换，而变换前后范数不变，且是可逆正交变换，通俗讲就是保持长度不变的一种坐标变换。量子计算机的工作原理如图 5-20 所示。

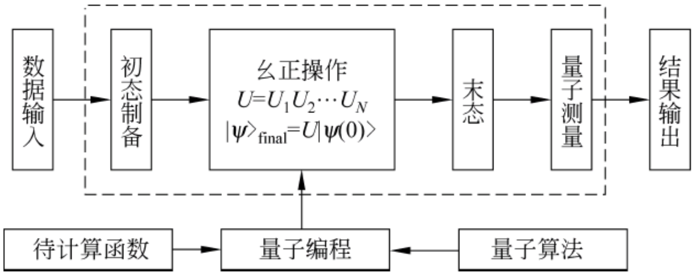

数据输入
初态制备
幺正操作
$U=U_1U_2\cdots U_N$
$|\psi\rangle_{\mathrm{final}}=U|\psi(0)\rangle$
末态
量子测量
结果输出
待计算函数
量子编程
量子算法

图 5-20　量子计算机的工作原理

所不同的是，电子计算机所用的电子存储器，在某个时间只能存一个数据，它是确定的，操作一次就把一个比特变成另一个比特，实行串行运算模式；而量子计算机利用量子性质，一量子比特可以同时存储两个数值，N 量子比特可以同时存储 2^N 个数据，操作一次会将这个 2^N 个数据变成另外一个 2^N 个数据，以此类推，运行模式为一个 CPU 的并行运算模式，运行操作能力指数上升，这是量子计算机来自量子性的优点。量子计算本来就是并行运算，所以说量子计算机天然就是“超级计算机”。

要想研制量子计算机，除了要研制芯片、控制系统、测量装置等硬件外，还需要研制与之相关的软件，包括编程、算法、量子计算机的体系结构等。

一台量子计算机运行时，数据输入后，被编制成量子体系的初始状态，按照量子计算机欲计算的函数，运用相应的量子算法和编程，编制成用于操作量子芯片中量子比特幺正操作变换，将量子计算机的初态变成末态，最后对末态实施量子测量，读出运算的结果。

一台有 N 量子比特的量子计算机，要保证能够实施一个量子比特的任意操作和任意两个量子比特的受控非操作，才能进行由这两个普适门操作的组合所构成的幺正操作，完

成量子计算机的运算任务。这是量子芯片的基本要求。如果要超越现有电子计算水平，需要多于1000量子比特构成的芯片，目前还没有这个能力做到。这种基于量子图灵机的标准量子计算是量子计算机研制的主流。

除此之外，还有其他量子计算模型，如单向量子计算、分布式量子计算，但其研制的困难并没有减少。另外，还有拓扑量子计算、绝热量子计算等。

由于对硬件和软件的全新要求，量子计算机的所有方面都需要重新进行研究，这就意味着量子计算是非常重要的交叉学科，是需要不同领域的人共同来做才能做成的复杂工程。

3. 把量子计算机从“垃圾桶”捡回来的量子编码与容错编码

实现量子计算机最困难的地方在于，这种宏观量子系统是非常脆弱的，周围的环境都会破坏量子相干性（消相干），一旦量子特性被破坏将导致量子计算机并行运算能力基础消失，变成经典的串行运算。

所以，早期许多科学家认为量子计算机只是纸上谈兵，不可能制造出来。直到后来，科学家发明了量子编码。

量子编码的发现等于把量子计算机从“垃圾桶”里又捡回来了。

采用起码5量子比特编码成1个逻辑比特，可以纠正消相干引起的所有错误。

不仅如此，为了避免在操作中的错误，使其能够及时纠错，科学家又研究容错编码，在所有量子操作都可能出错的情况下，它仍然能够将整个系统纠回理想的状态。这是非常关键的。所以，我们的目标就是研制大规模具有容错能力的通用量子计算机。

4. 量子计算机的量子芯片

量子芯片的研究已经从早期对各种可能的物理系统的广泛研究，逐步聚焦到了少数物理系统。

20世纪90年代时，美国的科学家不知道什么样的物理体系可以做成量子芯片，摸索了多年之后，发现许多体系根本不可能最终做成量子计算机，所以他们转而重点支持固态系统。

固态系统的优点是易于集成（能够升级量子比特数目），但缺点是容错性不好，固态系统的消相干特别严重，相干时间很短，操控误差大。

2004 年以来，世界上许多著名的研究机构，如哈佛大学、麻省理工学院、普林斯顿大学、东京大学、Delft 大学等都投入了很大的力量，在半导体量子点作为未来量子芯片的研究方面取得一系列重大进展。最近几年，半导体量子芯片的相干时间已经提高到 200μs。

近几年，科学家使用各种方法把超导的相干时间尽可能拉长，到现在也达到了 100 多微秒。这花了 13 年的基础研究，提高了 5 万倍。

特别是，超导量子计算在某些指标上也表现更好，分别如下。

(1) 量子退相干时间超过 0.1ms，高于逻辑门操作时间 1000 倍以上，接近可实用化的下限。

(2) 单比特门和两比特门运算的保真度分别达到 99.94%和 99.4%，达到量子计算理论的容错率阈值要求。

(3) 已经实现 9 量子比特的可控耦合。

(4) 在量子非破坏性测量中，达到单发测量的精度。

(5) 在量子存储方面，实现超高品质因子谐振腔。

美国从 20 世纪 90 年代到现在，在基础研究阶段超导领域的突破，已经引起了企业的重视。美国所有重大的科技公司，包括 Microsoft、Apple、Google 等公司都在量子计算机研制领域投入了巨大的力量，以期全力争夺量子计算机这块“巨大的蛋糕”。

其中，最典型的就是 Google 公司在量子计算机领域的布局，它们制订了一个计划：做到 50 量子比特，定这个目标是因为，如果能做 49 量子比特，在大数据处理等方面，就远远超过了电子计算机所有可能的能力。

量子计算现在正处于从晶体管向集成电路过渡阶段，如图 5-21 所示。

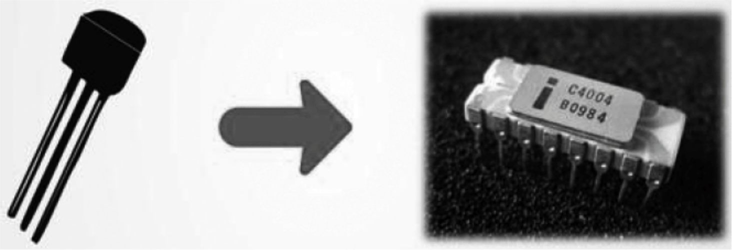


图 5-21　量子计算现在正处于从晶体管向集成电路过渡阶段

5.5.4　合久必分：IT世界顶级高手的竞争

1. Microsoft公司发布量子编程语言 5年内或推工作机

Microsoft、Google、IBM及一些小型专业化公司都在开发量子计算机，从理论上讲，量子计算机比现有计算机强大很多。Microsoft公司最近表示，它已经找到一种不同的方法，可以降低商用量子计算技术的出错率，让它更稳定。如果Microsoft公司所说的技术真的管用，也许可以推动量子计算快速走向商业化。

Microsoft公司已推出一门新的程序语言，名叫Q♯(念作Q Sharp)，这是一个工具，可以帮助编程人员为量子计算机编写软件。Microsoft公司还发布一些模拟器，让程序员在传统台式计算机上测试软件，或者通过Azure云计算服务测试。

2011年，D-Wave公司率先开始销售量子计算机，不过D-Wave公司的技术一直存在争议，因为计算机只能解决特定数学问题。Google、IBM公司的量子计算机更强大，更有可能帮助公司确立“量子霸权”地位，换言之，它们的技术可以解决复杂问题，这些复杂问题是标准超级计算机无法解决的。IBM和创业公司Rigetti Computing还为量子计算机开发了软件。

Microsoft公司不同，它想开发一台工作机。Microsoft公司的设计相当新颖，系统可以控制一种难以捉摸的粒子，这种粒子名叫Majorana(马约拉纳费米子)，几年前人类甚至还不确定这种粒子是否存在。在工程师的努力下，Microsoft公司已经接近达成控制粒子的目标，让粒子执行计算任务。研究人员认为5年之内Microsoft公司的量子计算机就可以进入市场。

人类也许可以用量子计算机开发药物和新材料，或者解决复杂的化学难题。Microsoft公司量子计算软件负责人认为，量子计算还有一个“杀手级应用”，可以用它寻找更高效的合成氨技术，用于化肥生产，目前这一处理过程要消耗全球3%的天然气。

一直以来，科学家不断研究量子计算，研究过程很漫长，至今仍然没有走出研究阶段，量子技术真的实用吗？大家意见不一。研究人员目前只能在几分之一秒的时间内让量子比特保持量子态。一旦量子比特脱离量子态，计算就会出错，这样一来使用量子计算机的好处就会被抹杀。

Microsoft 公司所使用的设计完全不同，Microsoft 公司把这种设计叫作“拓扑量子计算机”，从理论上讲它可以创造更稳定的量子比特。从出错的角度看，用 Microsoft 公司新设计制造的量子计算机比其他公司制造的量子计算机好 1000～10000 倍。

如果想将量子技术变成商用技术，减少或者修正量子计算错误是关键。Microsoft 公司的设计可以降低出错率，放在实际应用中也许更实用，即使量子比特少一些（可能不到 100 个）也会更实用。

2. IBM公司的量子计算机真的可以秒杀中国超算吗

回顾刚刚过去的 2017 年，中国超算再次 500 强夺冠，但美国也在追赶。同时，两国在量子计算机的研制上，也都在取得突破，竞争激烈。

量子计算领域 2017 年最大的新闻，莫过于 2017 年 11 月 12 日，IBM 公司宣布取得的重大进展。IBM 公司成功研发出 20 量子比特的量子计算机，成功建成并测试全球首台 50 量子比特的量子计算原型机，如图 5-22 所示。

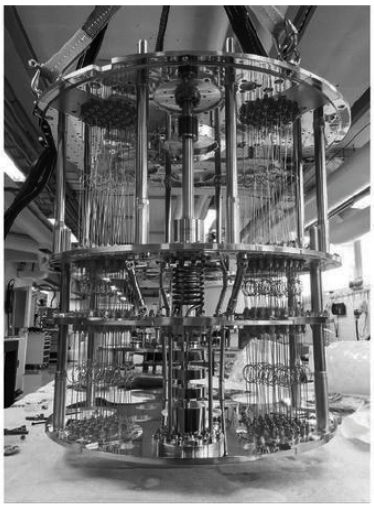


图 5-22　全球首台 50 量子比特的量子计算原型机

就在 2017 年 11 月，中国的超级计算机神威·太湖之光和“天河二号”再度蝉联 TOP 500 前两名。有媒体随即对 IBM 公司的量子计算机与神威·太湖之光超算进行比较，认为 IBM 公司的量子计算机可以秒杀神威·太湖之光。

2017 年 11 月 10 日，IBM 公司对外宣布，已经研发成功 20 量子比特的量子计算机，可在年底向付费用户开放，同时，IBM 公司还成功开发了一台 50 量子比特的原型机，但是 IBM Q 研究人员表示，量子比特数量增加只是一方面，处理的量子比特数越多，量子比特之间的交互就会越复杂。因此，50 量子比特的原型机虽然有更多的量子比特，这些量子比特的叠加态、纠缠态也会造成错误率很高的结果，无法保证精度和保真度，所以它不见得会比 5 量子比特的计算机更实用、更强大。

除此之外，各个巨头还推出了一些量子计算机的开放平台，例如，IBM 公司在 2017 年推出了量子计算服务 IBM Q 系统（20 量子比特量子计算云服务，如图 5-23 所示），这个系统的前身是 IBM 公司在 2016 年开放的 Quantum Experience 系统（5 量子比特量子计算云服务），这两个系统可以提供给用户试用 IBM 公司所造的 5 量子比特和 20 量子比特的量子计算机。除了 IBM，Microsoft 公司也在 2017 年 12 月推出了自己的量子计算机开发包，可以让用户在其开放平台上，用专用量子计算机编程语言 Q＃进行编程。

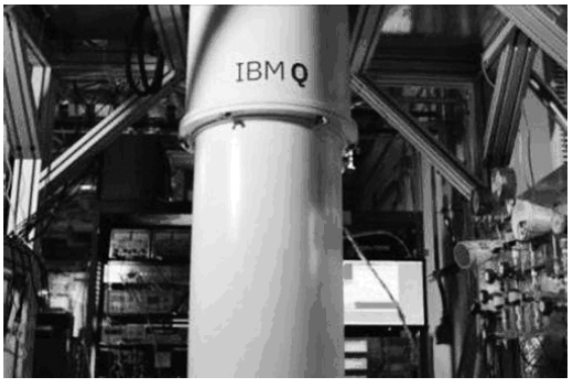


图 5-23　极度低温条件下工作的 IBM Q 量子计算机

3. 世界首台超越早期经典计算机的光量子计算机诞生

2017 年 5 月 3 日，世界上第一台超越早期经典计算机的光量子计算机在中国诞生，这标志着我国的量子计算机研究领域已迈入世界一流水平行列。据悉，该光量子计算机是由中国科学技术大学、中国科学院-阿里巴巴量子计算实验室、浙江大学、中国科学院物理所等协同完成参与研发的，是货真价实的“中国造”。光量子计算机原型如图 5-24 所示。

据介绍，经实验测试表明，该原型机的取样速度比国际同行类似的实验加快至少 24000 倍，通过和经典算法比较，也比人类历史上第一台电子管计算机和第一台晶体管计算机运行速度快 10～100 倍。

作为信息载体的量子比特的实现方式，是量子计算机研究中的一项关键性技术。优秀的量子比特实现方式一般需要满足几项特定的要求，如较为容易的物理载体的实现方式、容易的初态制备和操作、较长的相干时间等。

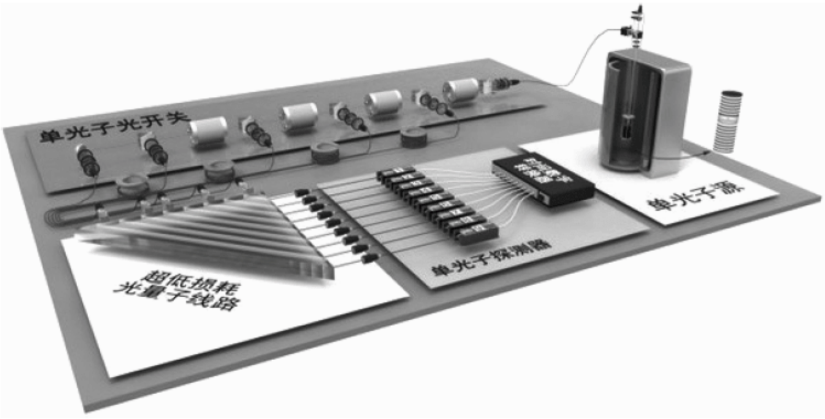


图 5-24　光量子计算机原型

目前，量子比特的实现方式主要有光子、离子阱、超导环、半导体量子结构等，基于这些不同物理载体实现的量子计算机各有优劣，如光子相干时间较长但难以观测和控制；超导环易于控制但相干时间极短；而离子阱虽然相干时间较长且易于控制，但由于需要频繁的激光操作，因此效率不高。

4. 量子计算机也存在致命的缺点

虽然从理论上来说，量子计算机的计算能力惊人，但是量子计算机也存在致命的缺点，主要有两点，这也是量子计算机一直发展缓慢的主要原因：第一是非常不稳定，需要低温运行；第二是精度差，错误率高。

成也萧何败也萧何，量子计算之所以能达到如此神速，是因为量子比特的叠加状态和量子纠缠，但与此同时，量子叠加和纠缠状态是极度脆弱的，不能受到一丁点儿干扰，量子计算机必须在极度低温条件下工作，低到什么程度呢？零下 273℃，这就好比拿一根很细很细的针顶起一个鸡蛋，稍有干扰，结果就会变得一片狼藉。

其次，因为量子比特的不稳定性，量子计算的精度也存在问题，保真度不高。保真度是什么呢？打个不恰当的比方，就好像你拿 100 块钱去银行柜台存了又取，取了又存，来回几次，最后取回来的钱却只有 60 块钱了，那保真度也就只有 60％。

就算这些问题都可以得到解决，量子计算机对于处理日常任务并没有什么用处，对于

普通人的生活影响不大。但在某些特殊领域里，量子计算机有传统计算机所不具有的能力，例如在化学和材料学里模拟分子结构，还有处理密码学、机器学习的一些问题，后文会详细说到，在此不赘述。

5. 实现量子计算机与量子通信为时尚早

量子力学诞生了一百多年，这是人类最成功的理论。因为有量子力学的诞生，人们才可能有激光、半导体以及更多先进技术。实际上，量子力学已经在人类生活中发挥着重要作用。

但是，以前由量子原理产生的器件，包括激光、半导体等都是经典器件，而量子信息技术是直接利用量子的性质研制出的量子器件，而不是经典器件。这个量子器件的功能要远远超越经典器件的物理极限，这就是量子信息技术带来的新时代的新技术。

量子力学的基本性质主要包含三个方面：首先，量子力学是叠加状态，所以从信息本身开始就是量子化的；其次，量子具有非局域性，而体现了非局域性的纠缠态是量子信息里非常重要的应用；最后，量子具有不可克隆性。

量子计算机实际上跟电子计算机一样，都是要解函数，不同的是量子计算机的处理操作用的是量子芯片。电子计算机用电子芯片去串行运算，用量子芯片替代它就会并行运算，所以量子计算机的速度就是量子性（即叠加性）导致的并行运算能力，相应的软件、编程也都做出相应的变化。

量子通信从学术上说是通过量子网络把量子信息传递过去。如果有两个量子网络，我们就可以构成联网，把所有的网络全连起来，就实现了一个量子云计算，这种功能将会比我们现在电子计算机为基础的计算网络功能强得多。

由于量子计算机、量子通信在技术突破以及产业化上有相当大的难度，因此，这两项技术还需要长时间的探索与研究，难以在短时间内实现。

6. 率先发力信息安全和传感器领域

量子信息技术可能会成为对人类带来最大冲击的新技术。量子技术可以应用在量子模拟机、量子计算机、量子通信、量子密码、量子传感等多个领域。相对于其他领域来说，量子技术将会率先在信息安全以及传感器领域得到应用。

量子信息出来以后，会对现在的保密系统产生很大的挑战。首先，现在的保密系统是利用数学的复杂度来确保保密信息的安全性，一个数学问题被解决了，它的安全也就被破解了。

在安全方面，量子计算机还比较遥远，但是量子密码是现在就可以用的。量子密码即量子保密通信。量子保密通信的安全性不靠数学计算的难度，而是靠物理定律，靠量子力学的不确定、不可克隆的基本原理，因而理论上没法破解，从而比现行安全技术更为可靠。

目前，量子密码稳定性等基本问题都已经解决。在某些领域，我国已经进行量子安全的产业化实验，技术已经接近于成熟。不过，由于缺乏量子中继技术，量子安全还只能在一个城市的城域网使用，两个城市之间还不能用。目前各地正在大力推进智慧城市，量子密码在单个城市应用实现突破，已经开启了一个很大的市场。

另外，传感器利用量子信息，还可以很容易传感各种物理量，这个比现在传感器的灵敏度和精度都有大幅度提高，而这也是在未来几年中将会面临的量子技术的应用。

现在有温度传感器、压力传感器和磁场传感器，人们现在正在做一个纳米级的显微镜，这些都是当前前量子传感器领域的研究热点。

总之，量子信息技术将会是人类发展的重要一环。

第6章

未来世界的神经中枢——量子通信

量子通信是指利用量子纠缠效应进行信息传递的一种新型的通信方式，是近20年发展起来的新型交叉学科，是量子论和信息论相结合的新的研究领域。

量子通信利用量子力学的基本原理或基于物质量子特性的通信技术。一个完整的量子通信系统以量子编码理论为基础，以特定的量子通信协议为核心，通过实现量子信号产生、调制和探测等关键技术，最终实现量子信息或经典信息的传送。量子通信最大的优点就是具有理论上的无条件安全性和高效性。

6.1 未来世界的神经系统

6.1.1 改变世界的新技术：量子通信

1. 什么是量子通信

量子通信主要涉及量子密码通信、量子远程传态和量子密集编码等。近年来，这门学科已逐步从理论走向实验，并向实用化发展。高效安全的信息传输日益受到人们的关注。基于量子力学的基本原理，并因此成为国际上量子物理和信息科学的研究热点。

量子通信如图6-1所示。

光量子通信主要基于量子纠缠态的理论，使用量子隐形传态（传输）的方式实现信息传递。根据实验验证，具有纠缠态的两个粒子无论相距多远，只要一个发生变化，另外一个也会瞬间发生变化。

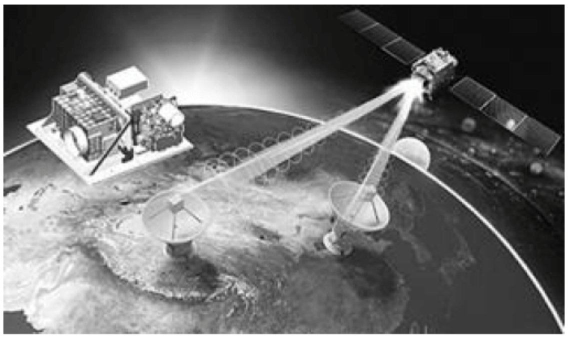


图 6-1　量子通信

利用这个特性实现光量子通信的过程如下：事先构建一对具有纠缠态的粒子，将两个粒子分别放在通信双方，将具有未知量子态的粒子与发送方的粒子进行联合测量（一种操作），则接收方的粒子瞬间发生坍缩（变化）。坍缩（变化）为某种状态，这个状态与发送方的粒子坍缩（变化）后的状态是对称的，然后将联合测量的信息通过经典信道传送给接收方，接收放根据接收到的信息对坍缩的粒子进行幺正变换（相当于逆转变换），即可得到与发送方完全相同的未知量子态。量子纠缠态理论结构如图 6-2 所示。

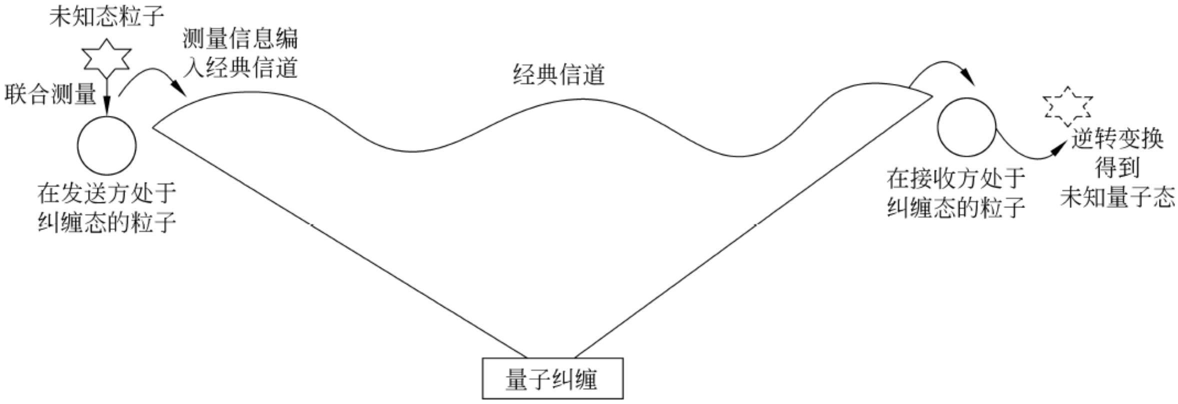

未知态粒子
测量信息编
入经典信道
联合测量
经典信道
在发送方处于
纠缠态的粒子
在接收方处于
纠缠态的粒子
逆转变换
得到
未知量子态
量子纠缠

图 6-2　量子纠缠态理论

经典通信与光量子通信相比，其安全性和高效性都无法与之相提并论。

2. 量子通信绝会不会“泄密”

量子通信绝不会“泄密”：其一，体现在量子加密的密钥是随机的，即使被窃取者截获，也无法得到正确的密钥，因此无法破解信息；其二，分别在通信双方手中具有纠缠态的2个粒子，其中一个粒子的量子态发生变化，另外一方的量子态就会随之立刻变化，并且根据量子理论，宏观的任何观察和干扰，都会立刻改变量子态，引起其坍缩。因此，窃取者由于干扰而得到的信息已经破坏，并非原有信息。

被传输的未知量子态在被测量之前会处于纠缠态，即同时代表多个状态。例如，一个量子态可以同时表示0和1两个数字，7个这样的量子态就可以同时表示128个状态或128个数字：0～127。光量子通信的这样一次传输，就相当于经典通信方式的128次。可以想象，如果传输带宽是64位或者更高，那么效率之差将是惊人的，以及更高。

3. 爱因斯坦的“幽灵”——量子纠缠的实证

量子通信具有高效率和绝对安全等特点，是国际量子物理和信息科学的研究热点。追溯量子通信的起源，还得从爱因斯坦的“幽灵”——量子纠缠的实证说起。

由于人们对纠缠态粒子之间的相互影响一直有所怀疑，几十年来，物理学家一直试图验证这种神奇特性是否真实。

1982年，法国物理学家艾伦·爱斯派克特和他的小组成功地完成了一项实验，证实了微观粒子“量子纠缠”的现象确实存在，这一结论对西方科学的主流世界观产生了重大冲击。

从笛卡儿、伽利略、牛顿以来，西方科学界主流思想认为，宇宙的组成部分相互独立，它们之间的相互作用受时空的限制（即是局域化的）。量子纠缠证实了超距作用的存在，它证实了任何两种物质之间，不管距离多远，都有可能相互影响，不受四维时空的约束，是非局域的，宇宙在冥冥之中存在深层次的内在联系。

在量子纠缠理论的基础上，1993年，美国科学家贝内特提出了量子通信的概念。量子通信是由量子态携带信息的方式，利用光子等基本粒子的量子纠缠原理实现保密通信的过程。量子通信概念的提出，使量子纠缠效益开始发挥其真正的威力。

1993年，在贝内特提出量子通信概念以后，6位来自不同国家的科学家，基于量子纠

缠理论，提出了利用经典与量子相结合的方法实现量子隐形传送的方案，即将某个粒子的未知量子态传送到另一个地方，把另一个粒子制备到该量子态上，而原来的粒子仍留在原处，这就是量子通信最初的基本方案。

量子隐形传态不仅在物理学领域对人们认识与揭示自然界的神秘规律具有重要意义，而且可以用量子态作为信息载体，通过量子态的传送完成大容量信息的传输，实现原则上不可破译的量子保密通信。

1997 年，在奥地利留学的中国青年学者潘建伟与荷兰学者波密斯特等人合作，首次实现了未知量子态的远程传输。这是国际上首次在实验上成功地将一个量子态从甲地的光子传送到乙地的光子上。实验中传输的只是表达量子信息的“状态”，作为信息载体的光子本身并不被传输。

经过 20 多年的发展，量子通信这门学科已逐步从理论走向实验，并向实用化发展，涉及的主要领域包括量子密码通信、量子远程传态和量子密集编码等。

6.1.2 众人拾柴火焰高：量子通信的类型

量子通信是指运用与量子相关的理论和方法，对信息进行传递和处理的技术。其信息的载体是微观粒子，如单个光子、原子或自旋电子等，与我们熟悉的经典通信相比，量子通信具有很多优势，例如，通信的无条件安全性，传递信息的高效性以及利用量子物理的纠缠资源等。根据工作机制的区别，可以将量子通信分为以下几类。

1. 量子保密通信（Quantum Private Communication, QPC）

量子保密通信是指通过量子力学理论基础构造协议与算法的一种通信手段，目前主要是基于量子密钥分发（Quantum Key Distribution，QKD）的量子保密通信。它是指相互通信的两者之间，利用量子力学的基本原理，将量子态作为信息的载体，通过量子信道传输，从而产生共享密钥的一种方法。它的安全性可以由海森伯不确定性原理与量子不可克隆定理来保证。

2. 量子隐形传态（Quantum Teleportation , QT）

量子隐形传态是指利用纠缠粒子对，将携带信息的光量子与纠缠光子对之一进行贝

尔态测量，将测量结果发送给接收方，接收方根据测量结果进行相应的酉变换，从而可恢复发送方的信息，这种方法又称为量子遥传、量子隐形传输，它传输的不再是经典信息而是量子态携带的量子信息，属于量子间接通信。

3. 量子安全直接通信（Quantum Secure Direct Communication, QSDC）

它是以量子态作为载体，利用量子特性，在收发两端进行直接安全的信息传输，并通过在系统中添加控制比特来检验信道的安全性。量子安全直接通信提高了通信的传输效率和实时性。

量子通信除上述三种形式之外，还有量子秘密共享（Quantum Secret Sharing，QSS）、量子认证（Quantum Authentication）、量子签名（Quantum Signature）、量子密集编码（Quantum Dense Coding）等多个分支。

在国际上，目前研究最多的是量子密钥分发和量子隐形传态，而它们也是研究其他量子通信的基础。其中，量子密钥分发又是量子通信中研究时间最长的一项技术，也是最接近于实用的技术。

6.2　云中漫步——量子隐形传态

6.2.1　通信神话：量子隐形传态的原理

1. 什么是量子隐形传态

量子隐形传态又称为量子遥传、量子隐形传输、量子隐形传送、量子远距传输或量子远传，是一种利用分散量子纠缠与一些物理信息的转换来传送量子态至任意距离的位置的技术。它是一种全新的通信方式。它传输的不再是经典信息而是量子态携带的量子信息，在量子纠缠的帮助下，待传输的量子态如同经历了科幻小说中描写的“超时空传输”，在一个地方神秘地消失，不需要任何载体的携带，又在另一个地方神秘地出现。

必须说明的是，量子遥传并不会传送任何物质或能量。这样的技术在量子信息与量子计算上相当有帮助。然而，这种方式无法传递传统的信息，因此无法使用在超光速的通信上面。量子遥传与一般所说的瞬间移动没有关系，量子遥传无法传递系统本身，也无法

用来安排分子以在另一端组成物体。

1）量子隐形传态的定义

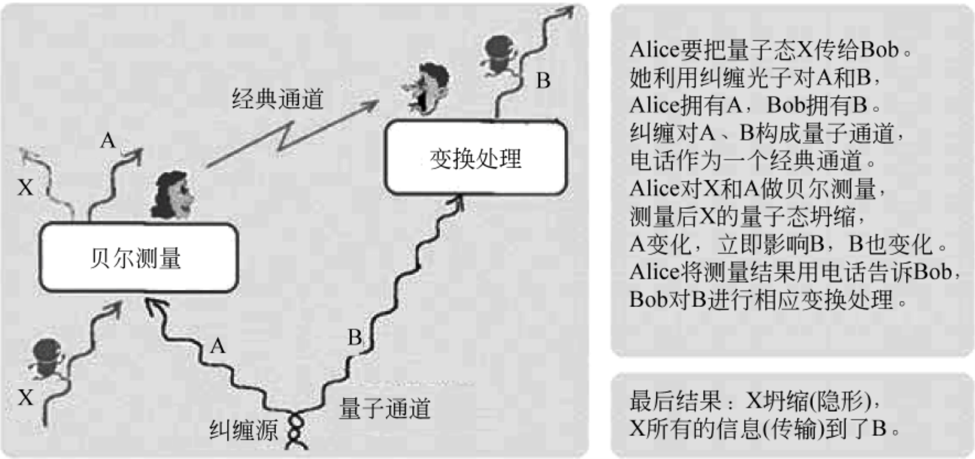
量子隐形传态是一种传递量子状态的重要通信方式，是可扩展量子网络和分布式量子计算的基础。在量子隐形传态中，遥远两地的通信双方首先分享一对纠缠粒子，其中一方将待传输量子态的粒子（一般来说与纠缠粒子无关联）和自己手里的纠缠粒子进行贝尔态分辨，然后将分辨的结果告知对方，对方则根据得到的信息进行相应的幺正操作。纠缠态预先分发、独立量子源干涉和前置反馈是量子隐形传态的三个要素。

通俗来讲，量子隐形传态是指将甲地的某一粒子的未知量子态，在乙地的另一粒子上还原出来。量子力学的不确定原理和量子态不可克隆原理，限制人们将原量子态的所有信息精确地全部提取出来。因此，必须将原量子态的所有信息分为经典信息和量子信息两部分，它们分别由经典通道和量子通道送到乙地。根据这些信息，在乙地构造出原量子态的全貌。

2）量子隐形传态过程

要实现量子隐形传态，首先要求接收方和发送方拥有一对共享的EPR对（即贝尔态），发送方对其所拥有的一半EPR对和所要发送的信息所在的粒子进行联合测量，这样接收方所有的另一半EPR对将在瞬间坍缩为另一状态（具体坍缩为哪一状态取决于发送方的不同测量结果）。发送方将测量结果通过经典信道传送给接收方，接收方根据这条信息对自己所拥有的另一半EPR对做相应幺正变换即可恢复原本信息。到乙地，根据这些信息，在乙地构造出原量子态的全貌。量子隐形传态的原理如图6-3所示。

与广为流传的说法不同，量子隐形传态必须借助经典信道才能实现，因此并不能实现超光速通信。在这个过程中，原物始终留在发送者处，被传送的仅仅是原物的量子态，而且发送者对这个量子态始终一无所知；接收者是将别的物质单元（如粒子）制备成为与原物完全相同的量子态，他对这个量子态也始终一无所知；原物的量子态在测量时已被破坏掉——不违背“量子不可克隆定理”；未知量子态（量子比特）的这种传送，需要经典信道传送经典信息（即发送者的测量结果），传送速度不可能超过光速（不违背相对论的原理）。



Alice要把量子态X传给Bob。
她利用纠缠光子对A和B，
Alice拥有A，Bob拥有B。
纠缠对A、B构成量子通道，
电话作为一个经典通道。
Alice对X和A做贝尔测量，
测量后X的量子态坍缩，
A变化，立即影响B，B也变化。
Alice将测量结果用电话告诉Bob，
Bob对B进行相应变换处理。

最后结果：X坍缩(隐形)，
X所有的信息(传输)到了B。

图 6-3　量子隐形传态原理

3）量子隐形传态的原理

量子隐形传态的基本原理，就是对待传送的未知量子态与EPR对的其中一个粒子实施联合贝尔基测量，由于EPR对的量子非局域关联特性，此时未知态的全部量子信息将会“转移”到EPR对的第二个粒子上，只要根据经典通道传送的贝尔基测量结果，对EPR的第二个粒子的量子态施行适当的幺正变换，就可使这个粒子处于与待传送的未知态完全相同的量子态，从而在EPR的第二个粒子上实现对未知态的重现。

6.2.2　原来是真的：量子隐形传态实验

1. 量子隐形传态研究成果

1997年，奥地利蔡林格小组在室内首次完成了量子隐形传态的原理性实验验证，成为量子信息实验领域的经典之作。2004年，该小组利用多瑙河底的光纤信道，成功地将量子隐形传态距离提高到了600m。但是，由于光纤信道中的损耗和退相干效应，传态的距离受到极大的限制，如何大幅度地提高量子隐形传态的距离成了量子信息实验领域的重要研究方向。

2007年，中国科学技术大学-清华大学联合研究小组开始在北京八达岭与河北怀来之间架设长达16km的自由空间量子信道，并取得了一系列关键技术突破，最终在2009年

成功实现了世界上最远距离的量子隐形传态，证实了量子隐形传态过程穿越大气层的可行性，为未来基于卫星中继的全球化量子通信网奠定了可靠基础。除此之外，联合小组还在该研究平台上针对未来空间量子通信需求开展了诱骗态量子密钥分发等多个方向的研究，取得了丰富的成果。

2012年8月，潘建伟等人在国际上首次成功实现百千米量级的自由空间量子隐形传态和纠缠分发，为发射全球首颗“量子通信卫星”奠定了技术基础。在高损耗的地面成功传输100km，意味着在低损耗的太空传输距离将能超过1000km，基本上解决了量子通信卫星的远距离信息传输问题。实验室情况如图6-4所示。

图6-4　中国实现量子通信100km隐形传态

2016年9月，中国科学技术大学的潘建伟教授、张强教授小组首先和清华大学合作开发了适合光纤网络传输的时间相位纠缠光子源，然后通过发展皮秒级的远程光同步技术和使用光纤布拉格光栅进行窄带滤波，成功地解决了两个独立光子源之间的同步和干涉问题；接着开发了针对远距离光纤所造成的延迟和偏振涨落以及实验系统的稳定性等问题的主动反馈系统；最后利用中国科学院上海微系统与信息技术研究所开发的超导纳米线单光子探测器，在合肥量子城域通信网络的30km链路上实现了满足纠缠态预先分发、独立量子源干涉和前置反馈，为未来可扩展量子网络的构建奠定了坚实基础。

2.量子隐形传态的科学意义

量子隐形传态是量子通信中最简单的一种。从事量子隐形传态实验，是实现全球量

子通信网络的可行性的前提研究。

量子通信拥有“绝不泄密”的本领，保护用户的通信安全。由于量子具有不可再分、不可复制的特性，如果在传输中受到干扰就会改变状态，接收方就可以发现。也就是说，除了在保护通信安全的前提下，量子通信还有“反窃听”的功能。如果有人窃听，信息就被偷听动作改变了，从而可以保证内容的绝密。

6.3　风靡全球——量子信道

量子通信和经典网络的融合需要解决物理层和组网技术、中继技术和通信应用技术等方面的相互融合问题。由于传统的光通信可能在未来很长一段时间内仍然是主要通信技术手段，因此，在光通信网络上实现量子通信网络，将是双方融合的基础。

6.3.1　未来世界的高速公路：量子信道

1. 什么是量子信道

量子信道指的是量子在里面传输不受影响的通道。由于电子带负电荷，在带正电荷的原子核的吸引下电子被束缚在原子内部。如果电子没有在一段时间内获得足够的能量，它就无法“逃离”原子核的束缚。但量子力学可以提供另一种方法，电子可以直接通过量子信道逃脱出来，这在物理学中称为隧穿效应。

打个比喻，这就像在大碗中放一个小石子，石子不会出来。除非石子的能量很大，大过碗壁的能量时，它就会从碗的上面跳出来。

但是量子物理学上有一个非常奇怪的效应，当碗壁足够矮，非常薄，即便碗壁的能量依然大于石子的能量，石子也会莫名其妙地跑出来，究竟它是怎么出来的谁也不知道，就像变魔术一样。这个跑出来的石子实际上是通过一个隧道跑出来的，这个通道就是量子信道。

德国科学家最新的实验成果就是利用百亿分之一秒的阿秒激光级脉冲攻击氖原子从而观察到了隧穿效应的全过程，而且证明了量子信道的存在。这就像我们看运动员跳高或者跳远的时候，眼睛并不能看清楚他们的身体在腾空过程中的每个细小变化，而通过慢

动作我们却可以把每一瞬间看清楚。

以上讲的是量子隧穿效应，与量子信道无关，请勿被误导。

2.是否有必要走一条全新的量子通信技术路线

从目前的实际情况来看，将量子通信网络与现有网络进行融合是其最优的发展战略。互联网在最初设计时并没有全面深入地考虑其自身的安全性，这是造成现今网络安全问题十分突出的主要原因之一。

多位专家认为，走量子通信与经典通信的融合发展之路是基于技术上的考虑，而不是基于经济层面的考虑。量子通信极强的保密性是基于量子密钥技术实现的，密钥也是基于量子的特殊性而研发的，而其他通信方面的技术与传统经典通信差异不大。

量子通信从原理走上小范围专用问题的实用化，是现在全世界都在努力的方向。这其中，十分重要的一方面就是要注意将量子通信与现有的传统通信相互融合，要善于借鉴现有的通信技术来发展量子通信技术。

多位专家认为，量子通信和经典网络的融合需要解决物理层和组网技术、中继技术和通信应用技术等方面的相互融合问题。由于传统的光通信可能在未来很长一段时间内仍然是主要通信技术手段，因此，在光通信网络上实现量子通信网络，将是双方融合的基础。

在现实的量子通信中，量子通信与现有传统通信的融合是一个相互“取长补短”的过程。量子通信不会完全取代现有的通信技术，而是在现有的技术上在物理层、网络层、应用层三方面将两者进行完美融合。

从物理层来说，可以从光源、探测器和信道方面考虑。在网络层方面，可以采取独立的信道和统一的网络结构，也可以用一根光纤既传递量子信号又传递经典信号。

在应用层面，量子通信可以同现有的互联网安全协议相结合，用量子密码来替换现有协议中的初始密码。这样既可以得到更可靠的安全性，也可以保持较高的通信速率。举例说，我们用量子密码生成种子密钥，然后用传统的经典方法进行扩张，这样既可以保证种子密钥的可靠安全，同时也可以保证较高的通信效率。

3.中国量子通信的发展成果

古人在信封上用火漆封口，信件一旦在运输途中被拆开，便会留下“泄密”的痕迹。不

难理解，量子密钥在量子通信中的作用比火漆更彻底：一旦有人试图打开信件，量子密钥会让信件自动销毁，并让使用者获知情况。由此来看，拥有这项技术成果对我国科学技术发展影响巨大。事实上，在量子通信领域，我国已是世界上最有发言权的仅有的几个国家之一，成果斐然。

在不需要中继的情况下，我国的量子通信技术可以在200多千米的距离上保证通信安全。在这一层面，我国是在世界上领先的。这项技术应用到实际层面上，安全距离可超过100千米，我国与美国、日本和欧洲的科技发达国家水平相当。

4. 量子通信潜在应用和未来前景

目前，随着量子通信的发展与进步，保密措施变得越来越复杂、越来越可靠。那么，量子通信的潜在应用和未来前景怎样？业内人士表示，量子通信在未来的国际竞争中将愈来愈激烈，人类将致力于将量子保密通信向更远距离和更大规模的广域网络发展。

量子通信对军事、国防、金融等领域的信息安全有着重大的潜在应用价值和发展前景。量子通信不仅可用于军事、国防等领域的国家级保密通信，还可用于涉及秘密数据、票据的政府、电信、证券、保险、银行、工商、地税、财政等领域和部门。

在国防和军事领域，量子通信能够应用于通信密钥生成与分发系统，向未来战场覆盖区域内任意两个用户分发量子密钥，构成作战区域内机动的安全军事通信网络。

此外，它还能够应用于信息对抗，改进军用光网信息传输保密性，提高信息保护和信息对抗能力；并能够应用于深海安全通信，为远洋深海安全通信开辟了崭新途径；利用量子隐形传态以及量子通信绝对安全性、超大信道容量、超高通信速率、远距离传输和信息高效率等特点，建立满足军事特殊需求的军事信息网络，为国防和军事赢得先机。

在国民经济领域和部门，量子通信未来可用于金融机构的隐匿通信等工程以及对电网、煤气管网和自来水管网等重要基础设施的监视和通信保障，促进国民经济的发展。

不过，量子通信技术的未来发展前景并不会一帆风顺，也会遇到各种挑战和困惑。据了解，量子信息技术包括两方面：量子通信和量子计算机。量子计算机目前仍然处在基础研究阶段，未能广泛实际应用。

6.3.2 能比光还快吗：光纤量子信道

一个物理量如果存在最小的不可分割的基本单位，我们就说这个物理量是量子化的，把这个最小单位称为量子。光子就是光量子，一束光至少包含一个光子，再少就不存在了。实验发现，原子中电子的能量不是连续变化的，而是只能取一些分立的值，也就是说，原子中的电子能量是量子化的。量子化是微观世界的普遍现象。

20 世纪上半叶（主要是从 1900 年到 1930 年），普朗克、爱因斯坦、德布罗意、玻尔、海森伯、薛定谔、狄拉克、玻恩和泡利等伟大的物理学家们创立了量子力学，这是我们目前对微观世界最准确的描述。

相对论几乎是爱因斯坦独力创造出来的，量子力学却是群星璀璨的产物。爱因斯坦在其中也发挥了非常重要的作用（提出光量子，这是他获得诺贝尔物理学奖的原因），但并不是最重要的。对量子力学最重要的两个贡献者是普朗克和海森伯（图 6-5 和图 6-6）。不过上面无论哪一位，都比在世的物理学家伟大多了，这是时代的垂青，个人无法改变。

图 6-5　普朗克

图 6-6　海森伯

1. 光量子假说

光量子假说是由爱因斯坦提出的大胆假设。他认为，光和原子、电子一样也具有粒子性，光就是以光速 c 运动着的粒子流，把这种粒子称为光量子。同普朗克的能量子一样，每个光量子的能量也是 $E=h\nu$，根据相对论的质能关系式，每个光子的动量为 $p=E/c=$

h/λ。

普朗克的量子假说提出后的几年内，并未引起人们的兴趣，爱因斯坦却看到了它的重要性。他赞成能量子假说，并从中得到了重要启示：在现有的物理理论中，物体是由一个个的原子组成的，是不连续的，而光（电磁波）却是连续的。

在原子的不连续性和光波的连续性之间有深刻的矛盾。为了解释光电效应，1905年爱因斯坦在普朗克能量子假说的基础上提出了光量子假说，解决了经典物理学无法解释的光电效应。

根据光量子假说，爱因斯坦顺利地推出普朗克公式，并且还提出了一个光电效应公式。

光量子假说成功地解释了光电效应。当紫外线这一类的波长较短的光线照射金属表面时，金属中便有电子逸出，这种现象被称为光电效应。它是由赫兹和勒纳德发现的。

光电效应的实验表明：微弱的紫光能从金属表面打出电子，而很强的红光却不能打出电子。也就是说，光电效应的产生只取决于光的频率而与光的强度无关。这个现象用光的波动说是解释不了的。因为光的波动说认为光是一种波，它的能量是连续的，和光波的振幅（即强度）有关，而和光的频率（即颜色）无关，如果微弱的紫光能从金属表面打出电子来，则很强的红光应更能打出电子来，而事实却与此相反。利用光量子假说可以圆满地解释光电效应。

按照光量子假说，光是由光量子组成的，光的能量是不连续的，每个光量子的能量要达到一定数值才能克服电子的逸出功，从金属表面打出电子来。微弱的紫光虽然数目比较少，但是每个光量子的能量却足够大，所以能从金属表面打出电子来；很强的红光，其光量子的数目虽然很多，但每个光量子的能量不够大，不足以克服电子的逸出功，所以不能打出电子来。

目前量子通信主要是以极化光纤为信息载体，采用纠缠光子对作为传输的量子信道。量子通信可以分为光纤量子通信和自由空间量子通信两个方向。

量子通信是利用纠缠光子对的非定域的关联、耦合特性，瞬时地完成信号的传输，且除非有密钥，信号不可破译。

最初的量子态分配是需要一个经典信道的，通过光纤或者大气等。由于大气的色散、随机涨落比较大，会引起量子纠缠态的退相干，所以实验中往往是用光纤来做的，如这些年国际和国内的实验。

2.量子通信协议

量子通信之所以具有普通通信达不到的安全性的原因之一就是其使用的协议。

（1）基于纠缠光子信号的量子通信协议。

（2）基于单光子信号的量子通信协议。

（3）基于连续变量信号的量子通信协议。

基于纠缠光子信号，Ekert91协议可以实现安全的量子密钥分发。通过量子纠缠，密钥在两地进行测量操作的瞬间直接生成，同时量子力学原理保证了任何对量子系统进行窃听的行为将不可避免地造成干扰，从而能够被通信双方发觉。本质上讲，连续变量量子密钥分发的安全性和单光子量子密钥分发一样，也是由不可克隆定理保证的。

图6-7所示是量子通信网络的协议分层，两边是量子通信终端，中间是量子交换机。

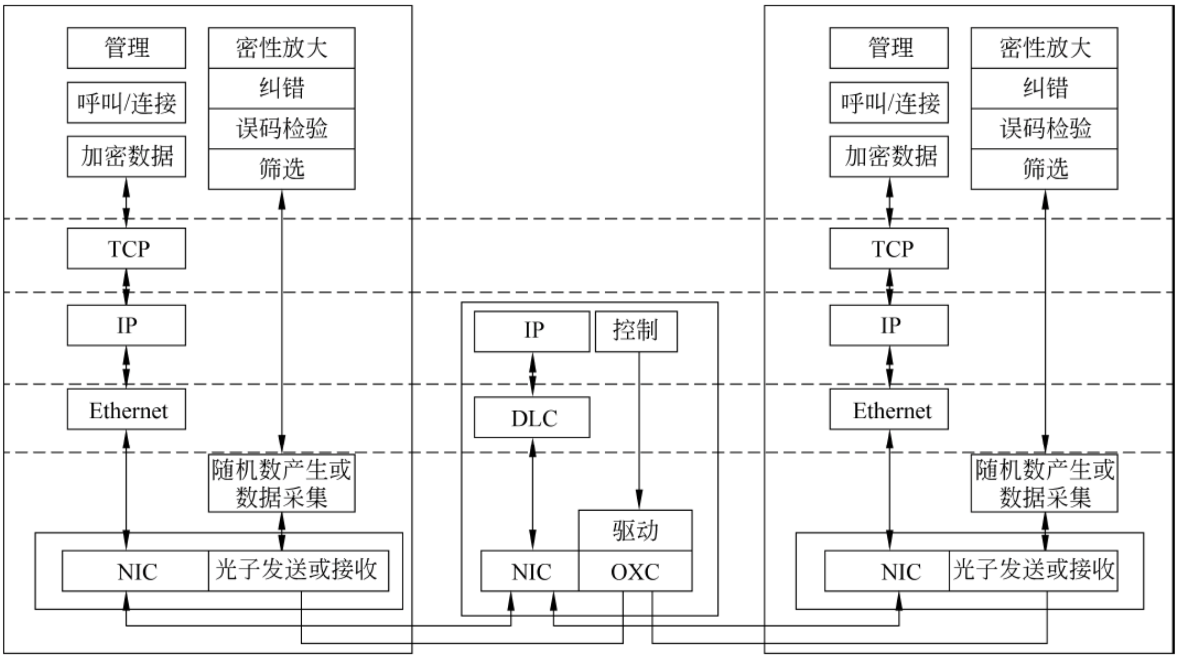

管理
呼叫/连接
加密数据
密性放大
纠错
误码检验
筛选
TCP
IP
Ethernet
随机数产生或数据采集
NIC
光子发送或接收
IP
控制
DLC
驱动
NIC
OXC
管理
呼叫/连接
加密数据
密性放大
纠错
误码检验
筛选
TCP
IP
Ethernet
随机数产生或数据采集
NIC
光子发送或接收

图6-7　量子通信网络的协议分层

两个用户均可作为发送方和接收方，其构成根据量子通信的具体形式和采用的方案而定。图中最上面的为应用层，在这一层会根据发送基和测量基的对比获得筛选密钥序列，进而经过误码检验获得最终密钥。也可以通过纠错降低量子信道的误码率，通过密性放大进一步提高数据的保密性。

3. 无线量子通信系统

目前最为成熟的量子通信技术是基于光纤信道实现的量子保密通信系统，但在无线量子通信中，基于自由空间信道的无线量子通信系统成果最为显著。

目前，自由空间量子通信实验还主要在地面大气环境中实施，此环境下的主要衰减机制为大气衰减和几何衰减。大气衰减来源于大气对信号光的吸收和散射；几何衰减是由于光具有一定的发散角，经过远距离传输后，信号光光斑将远大于接收端的接收口径，从而使接收端无法接收全部信号。

几何损耗是由于发射端发射的信号光存在一定的发散角，随着信号光传输距离的增加，信号光的光斑将逐渐扩大，而接收端的接收望远镜不可能无限制地提高接收口径，这就造成了接收端由于信号光光斑过大而无法完全接收而导致信号光损耗。由于光束的光斑尺寸会随着传输距离的增加而增大，光束也逐渐发散。要使光束的发散角变小，可通过增大它的光腰（光束横截面最小的平面处）半径来实现，为了得到扩大了的光腰，就需要先将光束扩束，一般情况下采用望远镜系统来达到扩束的目的。

6.3.3　太空通信：自由空间量子信道

量子通信是基于量子力学原理的通信方式，由于量子的先天特性，量子通信具有其他通信方式无法比拟的安全性。从20世纪80年代量子通信的提出，到今天量子通信已经可以实现百千米传输，量子光纤以及短距离自由空间传输技术不断地取得进步，但由于光纤的构建受到地理条件的限制，并且陆上自由空间量子通信的距离有限，无法实现长距离量子通信。

对于未来建立全球量子通信网的设想，量子通信的研究必须解决传输距离短，传输过程受外界地理条件影响大的缺陷。

卫星通信技术在当今信息社会已经得到很好的应用，卫星通信利用卫星与地面建立通信网络，使得通信范围大大提高，通信的时效性也得到改善。利用卫星来分发单光子（或纠缠光子对）的方法为远程量子通信网络提供了一种独特的解决方案，这将克服现有的光纤和陆上自由空间链路所带来的距离限制，实现真正意义上的全球量子通信。

量子科学实验卫星是中国科学院空间科学战略性先导科技专项于2011年首批确定的五颗科学实验卫星之一，旨在建立卫星与地面远距离量子科学实验平台，并在此平台上完成空间大尺度量子科学实验，以期取得量子力学基础物理研究重大突破和一系列具有国际显示度的科学成果，并使量子通信技术的应用突破距离的限制，向更深的层次发展，促进广域乃至全球范围量子通信的最终实现。

量子科学实验卫星专项的主要科学目标：进行星地高速量子密钥分发实验，并在此基础上进行广域量子密钥网络实验，以期在空间量子通信实用化方面取得重大突破；在空间尺度进行量子纠缠分发和量子隐形传态实验，开展空间尺度量子力学完备性检验的实验研究。

为实现科学目标，将借助卫星平台，在广域范围开展四项重要的科学实验。

1. 星地高速量子密钥分发实验

该实验室将在高精度捕获、跟踪、瞄准系统的辅助下，在实现地面与卫星之间建立超远距离的量子信道的基础上，进行卫星与地面之间、基于诱骗态和基于纠缠的量子密钥生成与分发，实现卫星与地面之间以量子密钥为核心的绝对安全的保密通信实验。

2. 广域量子通信网络实验

该实验将在实现高速星地量子密钥分发的基础上，与两个光学地面站及其附属的两个局域光纤量子通信网络相结合，通过卫星中转的方式组建真正意义上的广域量子通信网络。

3. 星地量子纠缠分发实验

在该实验中，卫星上的量子纠缠光源同时向两个地面站分发纠缠光子，在完成量子纠缠分发后，对纠缠光子同时进行独立的量子测量。通过对千千米量级量子纠缠态的观测，开展空间尺度量子力学完备性检验的实验研究。

4. 地星量子隐形传态实验

该实验将在量子存储的帮助下，探索卫星与地面之间远距离的真正意义及量子隐形传态的可行性，在类空间条件下完成量子力学非定域性的实验检验。地星量子隐形传态实验示意图如图 6-8 所示。

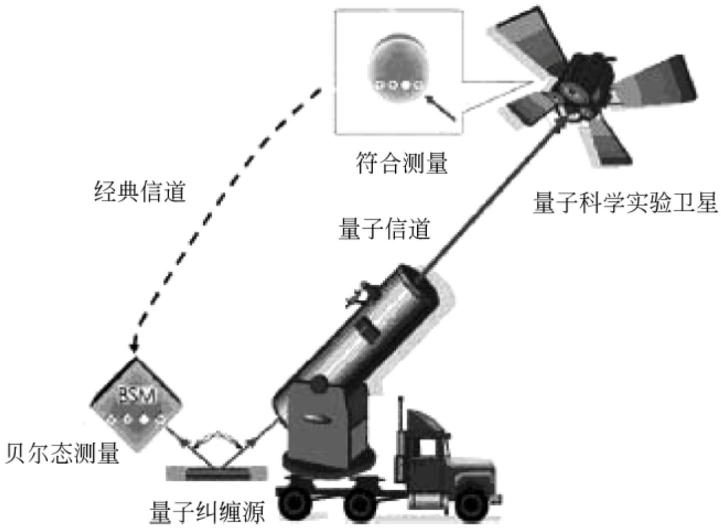


图 6-8　地星量子隐形传态

6.4　给互联网插上量子的翅膀——量子通信

6.4.1　通向未来的网络：量子通信网络的体系结构

一个典型的量子通信系统包括量子信源、量子信道和量子信宿三个主要部分。量子信源产生消息并发送出去；量子调制将原始消息转换成量子态形式，产生量子信号；量子信宿是消息的接收者，量子解调将量子态的消息恢复成原始消息；其余都属于量子信道范畴。另外通常还有辅助信道，是指除了传输信道以外的附加信道，如经典信道，主要用于密钥协商。

典型的量子通信系统组成如图 6-9 所示，量子通信系统的结构与作用如表 6-1 所示。

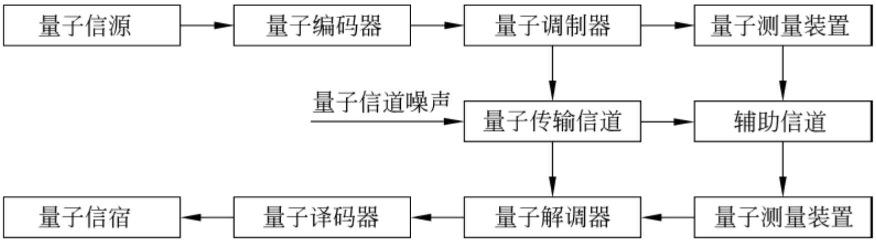

量子信源
量子编码器
量子调制器
量子测量装置
量子信道噪声
量子传输信道
辅助信道
量子信宿
量子译码器
量子解调器
量子测量装置

图 6-9　典型的量子通信系统

表 6-1　量子通信系统的结构与作用

结　　构	作　　用
量子信源	将要传输的信息转换成量子比特流
量子编码器	对量子比特流进行编码,进行数据压缩或加入纠错码对抗噪声
量子调制器	使量子信息的特性与信道特性匹配
量子测量装置	通过量子操作得到调制前的量子信息
量子传输信道	传送量子信号
辅助信道	经典信道及其他附加信道
量子信道噪声	环境对量子信号的影响
量子译码器	把量子比特转化成经典信息
量子信宿	量子信息接收方

根据信息传递机理,量子通信技术分为基于单光子信道的量子通信和基于纠缠对的量子通信。量子通信的不同传输对比如表 6-2 所示。

表 6-2　量子通信不同传输对比

比较项	基于单光子信道的量子通信	基于光子纠缠对的量子通信
机理	与经典通信相同	利用粒子纠缠特性脱离实物的隐形传递机制
信息载体	单光子	纠缠光子对
传递信道	光纤、自由空间光(FSO)等物理信道	光纤、自由空间

续表

	基于单光子信道的量子通信	基于光子纠缠对的量子通信
特点	具有经典通信无法提供的严格安全性	信息传递理论上可超光速，与距离无关，但由于需要经典信息作为测量辅助，获取信息的速度并未超光速； 具有经典通信无法提供的严格安全性
应用方式	量子安全直接通信；量子密钥分发；量子机密共享	量子隐形传态；量子纠缠密钥分发

根据通信系统工作原理，量子通信的关键技术可分为量子密钥分发、量子隐形传态、量子安全直接通信、量子机密共享等。

1. 量子密钥分发

量子密钥分发(QKD)是指利用量子状态作为信息加密和解密的密钥。量子密钥分配以量子态为信息载体，基于量子力学的测不准关系和量子不可克隆定理，通过量子信道使通信收发双方共享密钥，是密码学与量子力学相结合的产物。QKD 技术在通信中并不传输密文，只是利用量子信道传输密钥，将密钥分配到通信双方。其基本通信结构如图 6-10 所示。

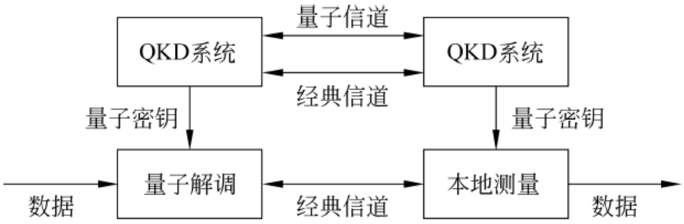


图 6-10　QKD 量子密钥分发系统结构图

目前，各国学者在理论上已经提出几十种量子密钥分配方案，根据信号源的不同大致可分为三类：基于单量子的量子密钥分配方案、基于量子纠缠对的量子密钥分配方案和基于单量子与量子纠缠对的混合量子密钥分配方案。

现有的量子密钥分发技术可以实现实验室状态下 200km 以上的量子通信，再辅以光开关等技术，还可以实现量子密钥分发网络。目前，开始产业化的是量子密钥分配，例如，“京沪量子通信干线”“沪杭量子通信干线”以及陆家嘴量子通信金融网等。

2 量子隐形传态

量子隐形传态是量子信息领域的典型应用，又称为量子离物传态或量子远程通信。与传统的通信方案相比，量子隐形传态技术是利用量子纠缠理论，通过一对EPR纠缠对实现远距离量子信息传输，不需要直接传输量子比特信息而实现量子纠缠态的转移。量子隐形传态理论在实验中得到了成功实现，并成为当前量子通信系统的重要理论基础，其技术系统结构图如图6-11所示。

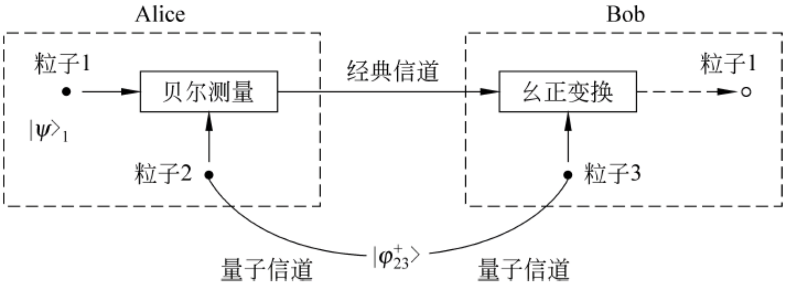


图6-11　量子隐形传态技术系统结构图

发送者Alice要将粒子1传递给接收者Bob，需要分别经过经典信道和量子信道两部分的传输过程，其具体步骤如下。

（1）Alice在发送端对所持有的粒子1和粒子2进行联合贝尔测量，使其坍缩到四个贝尔基中的一个。Alice将测量得到的结果通过经典信道传给Bob。当Alice完成测量工作后，Bob手中的粒子3立刻坍缩到所对应的量子态上。

（2）Bob根据所接收到结果对手中的粒子3的量子态进行相对应的幺正变换，得到粒子1初始未知态的一个精确备份，完成了未知态的传输。从量子隐形传态的传输过程可以看出，粒子1在Alice手中已经遭到破坏，不可能通过通信信道传输到Bob处，Bob只是通过相应的幺正操作利用手中已有的粒子3实现对未知粒子1的再现，而不是对粒子1的复制，所以量子隐形传态理论并不违背量子不可克隆定理。

量子隐形传态的工作原理使得需要传输的未知量子态不受传输信道的影响，并且该系统能够较好地抵御外界窃听或攻击，这使得该理论在量子通信网络中得到了广泛应用，尤其是涉及到量子态的转移、中转等技术上有着很好的应用前景。

3. 量子安全直接通信

量子安全直接通信是指通信双方以量子态为信息载体，基于量子力学相关原理及量子特性，利用量子信道，在通信收发双方之间安全地、无泄露地直接传输有效信息，特别是机密信息的通信技术。

QSDC是量子通信技术的一个重要分支，主要用于直接传输机密信息。通信的收发双方无须事先建立安全密钥，就可以直接通过量子通道进行信息传输。QSDC与量子密钥分发的根本区别在于在量子信道中直接传递秘密信息，安全性要求比量子密钥分配高，但总体而言，QSDC方案还存在非实时及其量子信道信息所需要的纠缠态、量子存储等技术还不成熟的问题。

下面以高效两步方案为例说明QSDC的原理。

在高效两步方案中，Alice随机制备 n 个处在某一贝尔态上的纠缠光子对，并将这个纠缠光子对分成两个序列，从每一纠缠光子对中挑出一个光子A，组成一个光子序列，而上述每一纠缠光子对中的另一个光子就可以组成另一个光子序列。Alice先将量子数据块发给信息接收者Bob。Bob接收到这个粒子序列后，随机地选择部分粒子进行安全性检测，与Alice进行安全分析。

在确保第一步通信安全以后，通信双方就建立了一个安全的量子纠缠信道。Alice将量子数据块发送给Bob。这样，Bob就得到了Alice的编码纠缠态。对这些纠缠态进行联合的纠缠态测量就可以读出态的信息，从而获取Alice加载的信息。通信双方就以安全的方式传输了信息。

高效两步方案中的ILBED(Information Leakage Before Eavesdropping Detection，窃听检测前的信息泄露)是通过对分步传输的量子数据块进行抽样测量得以避免的。对由EPR对中的第一个粒子组成的块进行随机抽样测量后，可以确定该粒子块的安全性，而这些粒子只是纠缠对中的一个粒子组成的，因此，不携带粒子对的整体状态，窃听者虽然可以窃听，但是得不到粒子对的状态信息，而窃听者的窃听则造成误码检测中的误码率升高，从而被合法通信双方探测。如果发现窃听，则将终止通信，而此时窃听者由于没有得到整个粒子对，得不到任何秘密信息，从而就避免了ILBED。

高效二步方案量子安全直接通信示意图如图 6-12 所示。

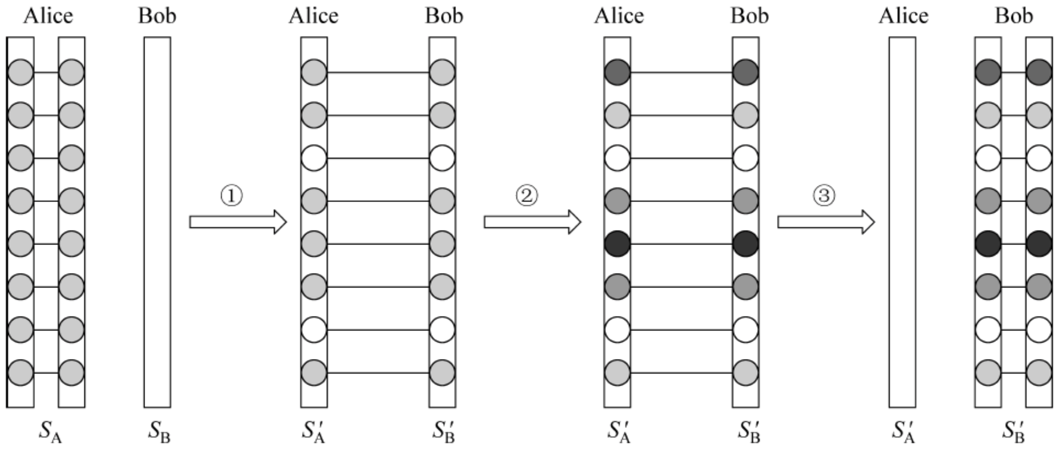


图 6-12　高效二步方案量子安全直接通信示意图

4. 量子机密共享

量子机密共享是传统的机密共享在量子通信中的运用和发展，传统的机密共享旨在对重要的密钥进行安全保护，使即便部分或全部密钥被第三方窃取也难以恢复出真实的密钥。其主要实现思路是，将原始密钥分割成多份，然后将多份密钥分别发给多个用户，每个用户都只能获取一份或多份密钥份额，只有在多个密钥分享者的合作下，才能恢复出原始的密钥，不能满足上述条件的共享者将无法得到全部的密钥。通过使用机密共享方案，可以在分享机密信息的同时，防止不诚实用户的破坏企图。

量子机密共享是多个通信方之间通过多量子纠缠态实现的量子通信，但现实应用技术难度大，还基本处于理论研究阶段。

6.4.2　未来世界的互联互通：量子通信网络中的交换技术

通信网络中通常都有一个核心节点，充当控制器，在某一时刻，控制器往往只能与一个用户进行通信，这在许多情况下无法满足多用户的需求，尤其是实时需求。采用交换技术是解决这一问题的可行途径。

与经典网络相同，量子通信网络交换的目的也是为了实现多个用户之间的任意互连，

从而节省骨干网络资源，实现用户共享中继线或是骨干线路。由于量子态不可克隆定理的限制，使得经典交换方法应用于量子通信中有许多技术障碍，例如，存储量子态的同时保持量子特性不变等。这里主要介绍几种目前可行的量子交换方案：空分交换、波分交换以及基于量子交换门的交换，后两者主要用于小规模的用户互连。

1. 空分交换

空分交换是指通过改变光量子脉冲的传输通道，使得在两个用户之间建立量子信道的技术。量子空分交换机的结构如图 6-13 所示。

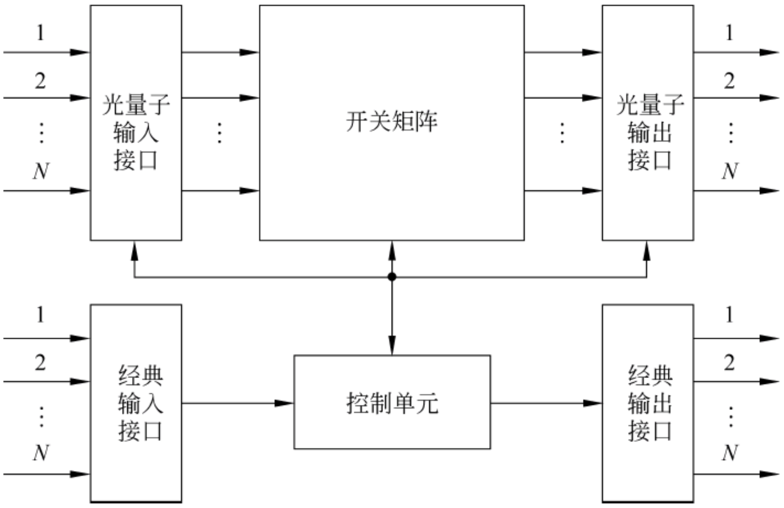


图 6-13　量子空分交换机的结构示意图

图 5-13 中，量子空分交换机由开关矩阵、输入输出接口以及控制单元组成。其中，开关矩阵的作用是实现光量子传输通道的切换。光量子输入接口将接收到的光量子信号送至开关矩阵，光量子输出接口再将从开关矩阵中输出的光量子送往链路。控制单元的功能是负责接收并处理用户的呼叫/连接请求以及路由选择。量子空分交换控制单元的信息通过经典输入输出接口发送与接收。

量子空分交换机的关键在于开关矩阵，开关矩阵也称为交换网络，它的组成方式很多，典型的包括 Crossbar 结构、Banyan 结构、Benes 结构以及 Clos 结构等，以无阻塞 8×8 Benes 互连结构为例，如图 6-14 所示。

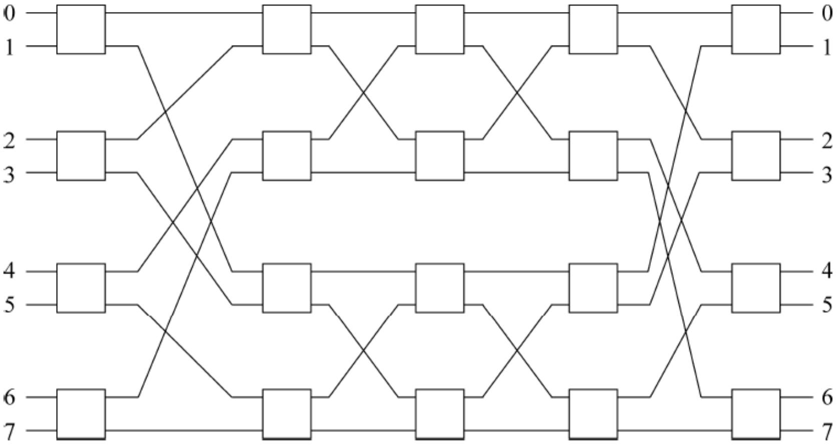

0
1
2
3
4
5
6
7
0
1
2
3
4
5
6
7

图 6-14　无阻塞 8×8 Benes 互连结构

在 Benes 网络中，从输入端到中间级可以自由选择，也就是说，任何一条通路都可以到达所需要的输出端，然而从中间级到输出端只能指定选择。

2. 波分交换

波分交换是通过光信号波长的不同来实行通路的技术。由于可以充分使用光的宽带特性，使得电控线路交换所无法完成的波分交换网络得以实现。波分交换的主要器材包括可调波长的滤波器以及波长变换器等。可调波长滤波器的作用是利用不同的波长来从多路光信号中进行选择。波长变换器的功能则是将变波长滤波器选出的光信号转为适合的波长之后再进行输出。其原理如图 6-15 所示，其基本单元就包括波分复用器、波分解复

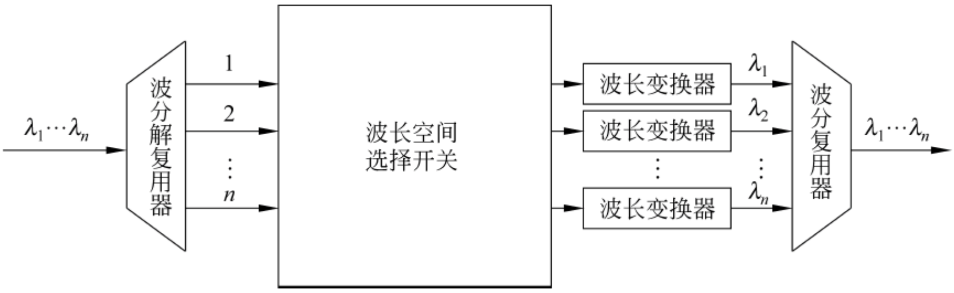

$\lambda_1 \cdots \lambda_n$
波分解复用器
1
2
⋮
n
波长空间选择开关
波长变换器
波长变换器
⋮
波长变换器
λ_1
λ_2
⋮
λ_n
波分复用器
$\lambda_1 \cdots \lambda_n$

图 6-15　波分交换结构示意图

用器、波长空间选择开关以及波长变换器。

由于当前的光量子通信网络主要是通过不同波长来区分不同的用户的，所以波分交换是一种可行的方案，其原理如图 6-16 所示。

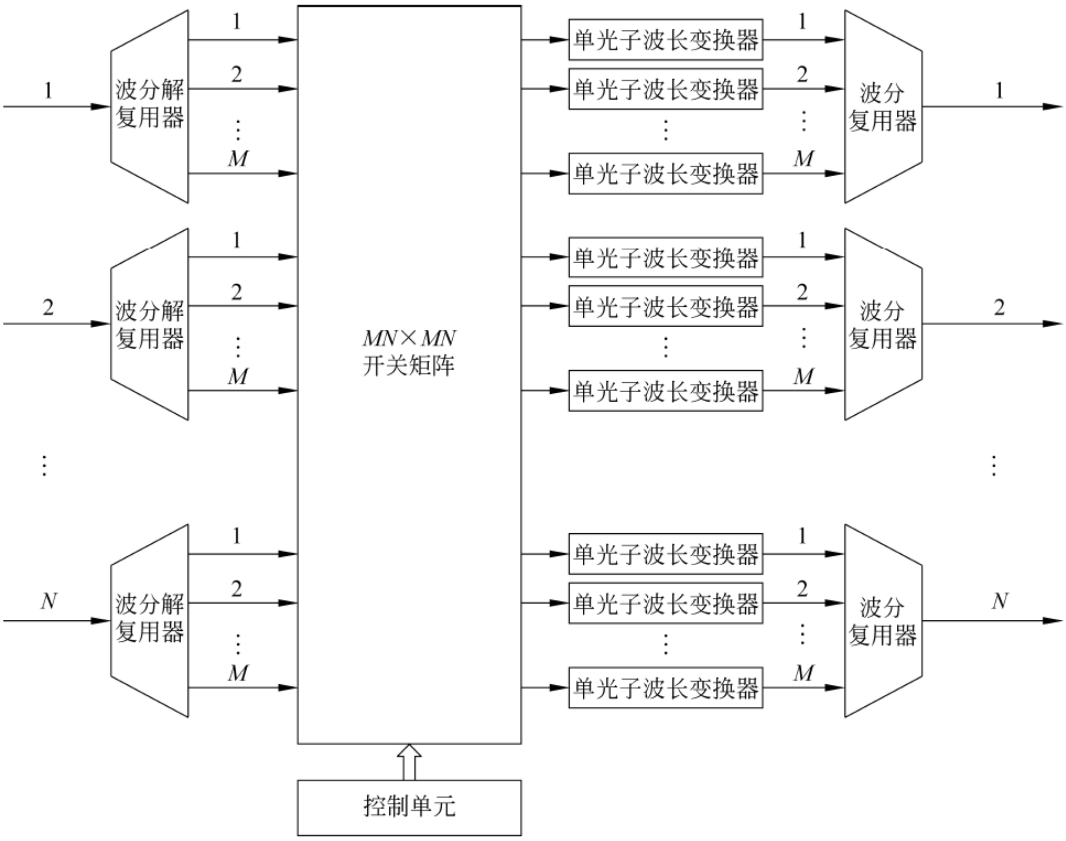

1
2
N
波分解复用器
1
2
M
MN×MN
开关矩阵
单光子波长变换器
波分复用器
控制单元

图 6-16　基于波长变换的波分交换原理图

图 6-16 中，N 路复用信号首先进入交换机，每一路都包含 M 个不同波长的光量子脉冲，之后通过解复用，分离出具有不同波长的用户信号，之后再进入开关矩阵，使其在控制单元的控制下进行选路，在通过指定的出口后，进入单光子波长变换器进行波长变换，当到达相应的波长后，再经过波分复用器进行合路。

在光量子波分交换系统中，单光子波长变换器是至关重要的器件，可以通过泵浦光与信号光的非线性作用来实现。其原理如图 6-17 所示，将泵浦光与信号光送进波分复用器

合路，再送进 PPLN（Periodic Polarization of Lithium Niobate，周期性极化的铌酸锂）晶体进行非线性作用，再通过一系列的滤光系统，包括三棱镜、小孔光阑以及滤波器对杂质进行滤除。最后使用单光子计数模块对波长变换后的光子进行探测。实际应用时需要合理地设计泵浦光线宽、功率以及晶体结构，从而在波长变换的同时保证量子态特性不会发生改变。

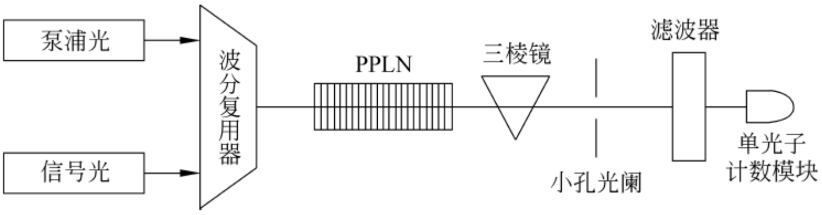

泵浦光
信号光
波分复用器
PPLN
三棱镜
小孔光阑
滤波器
单光子计数模块

图 6-17　单光子波长变换的原理示意图

3. 基于量子交换门的交换

量子交换门可以实现两个输入量子态之间的对换，如图 6-18 所示，其可以由三个受控非门组成。

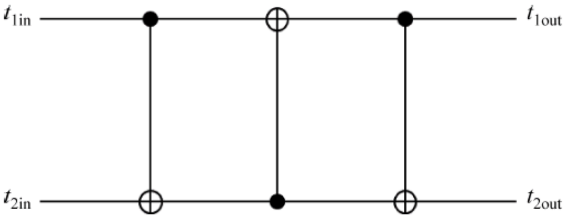

$t_{1\text{in}}$
$t_{1\text{out}}$
$t_{2\text{in}}$
$t_{2\text{out}}$

图 6-18　由受控非门构成的量子交换门

量子 Fredkin 门是在量子交换门之上增加了一个控制比特 c，当控制比特 c 是 1 时进行交换；当控制比特 c 是 0 时，不进行交换，如图 6-19 所示。

量子交换门与量子 Fredkin 门可以通过光学技术实现，由对光量子的操作，就变成了对光子偏振态的操作。量子 Swap 门如图 6-20 所示。

在图 6-20 中，半波片 HWP_1 的作用类似于一个非门，如果非门工作则实现量子态的对换，否则维持量子态不变。因此，可以使用一个受控非门来替代这个功能，并且根据控

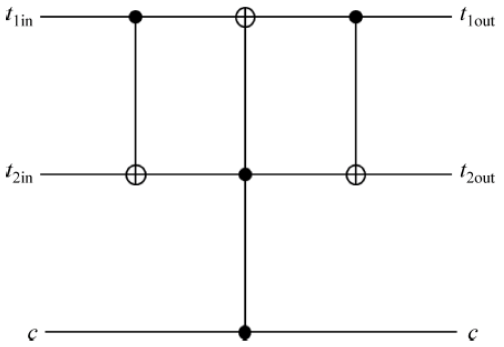
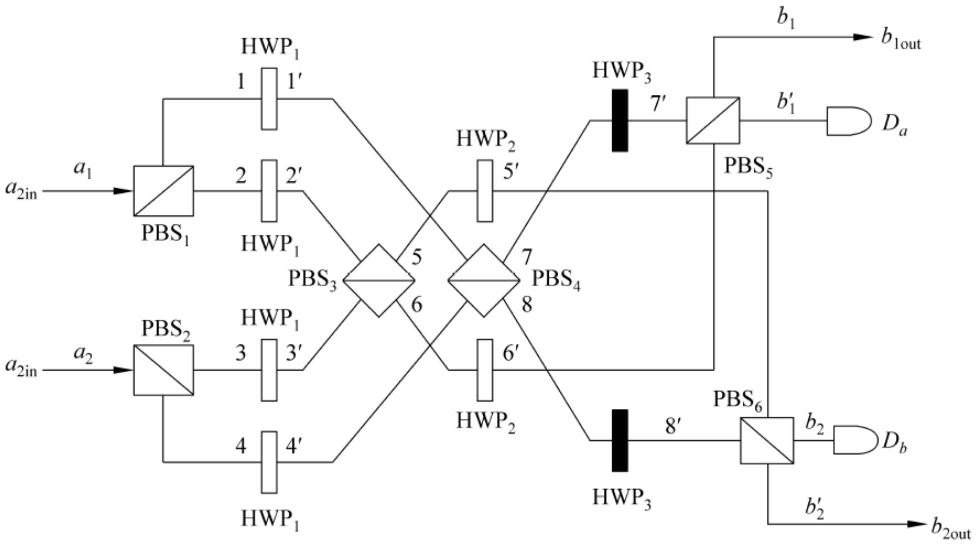

$t_{1\text{in}}$
$t_{1\text{out}}$
$t_{2\text{in}}$
$t_{2\text{out}}$
c
c

图 6-19　量子 Fredkin 门


b_1
$b_{1\text{out}}$
HWP_1
1
1′
HWP_3
7′
b'_1
D_a
HWP_2
PBS_5
a_1
$a_{2\text{in}}$
2
2′
5′
PBS_1
HWP_1
5
7
PBS_3
PBS_4
6
8
HWP_1
PBS_2
a_2
$a_{2\text{in}}$
3
3′
6′
HWP_2
PBS_6
8′
b_2
D_b
4
4′
HWP_1
HWP_3
b'_2
$b_{2\text{out}}$

PBS：偏振分束器；HWP：半波片；D：单光子探测器

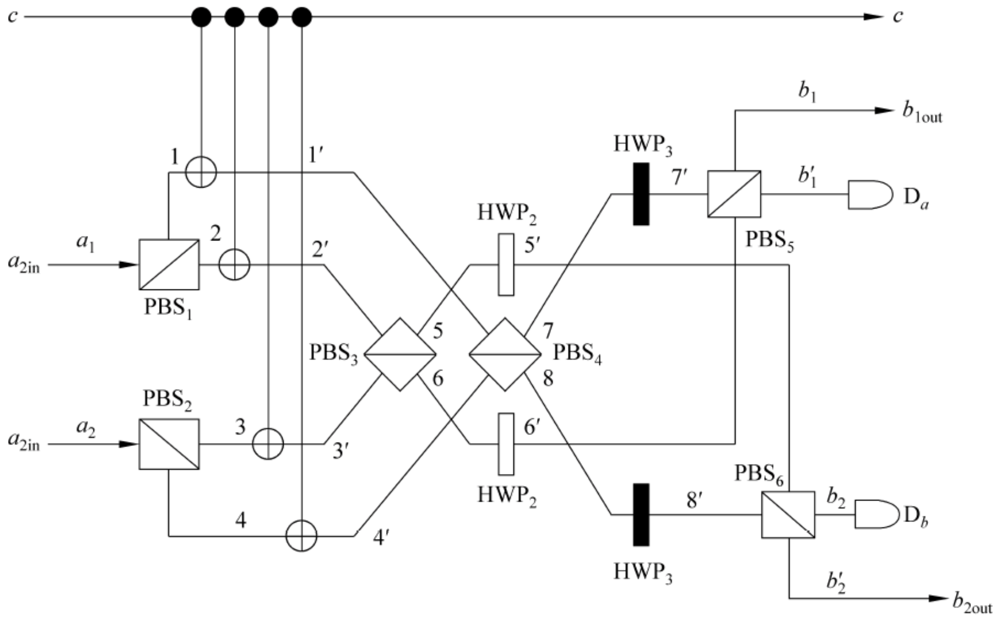
图 6-20　量子交换门的光学实现

制状态 c 的信息实现对换或者直通，即构成了量子 Fredkin 门，如图 6-21 所示。

4. 量子交换机结构设计

我们首先在基于偏振编码 BB84 协议上，建立了一个控制与传输相分离的三层量子通信网络体系结构，如图 6-22 所示。

在图 6-22 中，位于底层的传输平面将为量子通信提供量子信道，其主要是由量子传


c
c
1
1′
2
2′
3
3′
4
4′
a_1
$a_{2\text{in}}$
a_2
$a_{2\text{in}}$
PBS$_1$
PBS$_2$
PBS$_3$
PBS$_4$
PBS$_5$
PBS$_6$
5
6
7
8
5′
6′
7′
8′
HWP$_2$
HWP$_2$
HWP$_3$
HWP$_3$
b_1
$b_{1\text{out}}$
b_1'
D$_a$
b_2
D$_b$
b_2'
$b_{2\text{out}}$

PBS：偏振分束器；HWP：半波片；D：单光子探测器

图 6-21　量子 Fredkin 门的光学实现

输链路与量子交换模块两部分组成，由分布于各个节点设备当中，负责控制的部分构成控制平面，它的主要作用是让通信信令能够在各分布节点之间成功地传输，完成多个用户之间的呼叫连接控制，实现链路资源管理，为传输平面中量子信道的建立提供路由管理与用户接口。

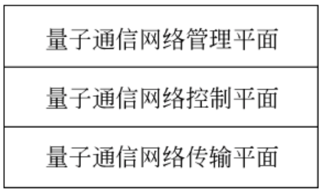

量子通信网络管理平面
量子通信网络控制平面
量子通信网络传输平面

图 6-22　量子通信网络体系结构

所以，整个控制平面可以看作一个用于控制传输平面量子通信设备的 IP 网络，控制平面的另一个作用是为量子通信提供经典辅助信道。管理平面由量子通信网络中各个节点设备的管理层一同构成，实现了管理功能的分布化。管理平面完成了一些更为高级的控制。

该网络的工作流程：当用户发起呼叫连接请求时，控制层会根据管理层的需要，依靠所知的平面拓扑信息建立端到端的连接，然后将控制消息发送到传输层，在传输层建立起

双方量子通信的物理链路，而其他的信息则通过经典信道进行选路、交换与呼叫连接管理。控制层的作用是保证链路通畅，直到本次通信结束后再释放链路资源，然后下一次通信请求到来时再次建立连接。

我们通过参考经典交换机的结构，设计了量子交换机，其结构如图 6-23 所示。

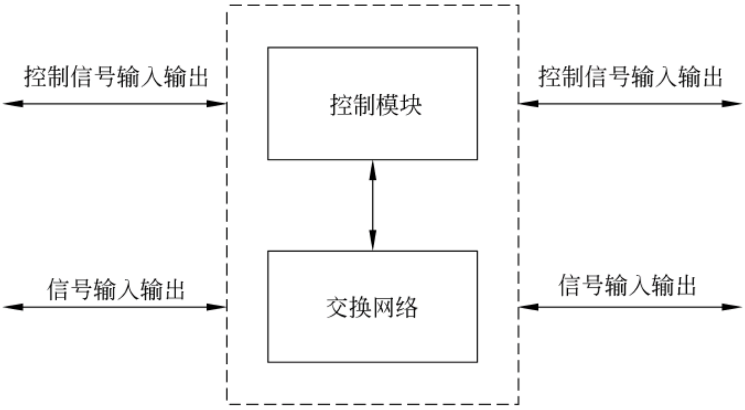


图 6-23 量子交换机的结构框图

在图 6-23 中，量子交换机的结构主要由控制模块、交换网络以及输入输出端口三部分组成。这里控制模块最为重要，它实现量子通信网络中控制平面上的功能，其中包含呼叫连接建立、链路资源管理、路由的建立与维护、管理平面与控制平面的连接、管理平面与传输平面的连接等功能并且为量子通信提供了 TCP/IP 网络作为辅助信道。交换网络和输入输出端口的作用则实现了传输平面以及接口的功能，为量子通信提供了物理信道。在此原理框图的基础之上，我们可以设计一个量子交换机的具体实现结构图，如图 6-24 所示。

在图 6-24 中，通过两层分立的形式组成交换机，按照功能将量子交换机划分为两个关键的模块：处于下层的是光路部分，即光交叉连接模块；处于上层的是电路部分，即交换控制和光交叉连接控制模块，其中又包括路由构造维护、呼叫连接控制、链路资源管理以及用户接口等各个子功能模块。

光交叉连接模块及其驱动电路作为交换网络，实现了传输平面的功能，为量子通信提供了量子信道。为了能够实现对量子信息进行交换，我们使用光开关搭建了一个全通的

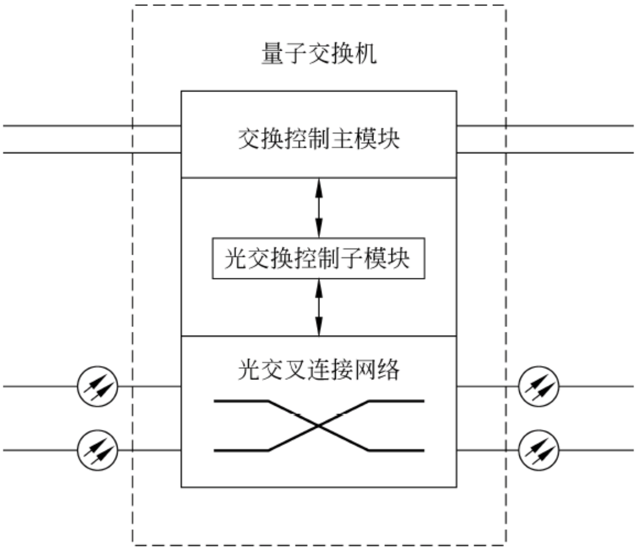


图 6-24　量子交换机实现结构图

交换网络，用以完成多个用户之间的全通通信网络传输平面的功能。交换控制模块实现了控制平面的功能，包括呼叫连接管理、链路资源管理、路由计算与维护等，同时交换模块也需要完成控制平面与传输平面连接的功能。

通过对比上面提到的量子通信网络结构与设计出的量子交换机，可以看出这个量子交换机基本可以满足量子通信网络的需求，下面主要研究量子交换机在控制功能上的软件设计以及改进。

5. 交换服务程序的设计与改进

建立一套基于硬件底层的软件系统，不仅可以实现交换机动态地更新光网络的拓扑、路由信息，收发各种指令、监控链路等，同时，还可以完成通过经典信道的信息交换、数据加密传输、密钥协商等工作。建立这个系统需要使用一定的信令，通过网络的控制面板实现用户的呼叫及通信任务，在用户与用户、用户与交换机之前建立、删除、查询、连接的平台，实现密钥协商和数据通信。

需要完成的工作如下：在呼叫过程中进行用户认证处理，执行相应操作，管理网络的监控及呼叫，完成连接的认证与信令传递；对用户进行识别，并实时管理链路资源，建立光

量子通道，成功搭建量子通信信道；支持多用户和静态、动态网络，方便地实现动态更新和用户扩展；协调通信数据机不同信道，实现经典信道及光量子信道的协同工作。

通过上述需求我们发现，路由控制及管理、呼叫连接控制、链路资源管理构成了量子交换机的控制部分，具体解决方法从以下三个方面入手。

1）路由信息管理

需要在量子交换机中加入路由资源信息数据库来记录网络拓扑、可达性等网络信息，当有用户加入或离开网络时，立即更新此数据库，并存储最新的路由交换信息。

2）路由控制及协议

在收到用户的呼叫请求之后，交换机要根据路由表查询目的用户，确定其连接路径，并在路由状态发生改变时及时更新。静态路由通过在本地IP路由表中显示和修改条目网络命令实现，只需用路由表设置路由规则，规定数据包流向。动态路由则是通过修改路由选择信息协议来实现的。

3）信道资源管理

通过专门的状态记录所有的信道工作及使用状况来实现量子信道工作状态的管理。完成呼叫连接相关处理以及通信数据管理收发双方的客户端。这里我们主要介绍交换控制程序的设计与实现。

量子交换机交换控制流程如图6-25所示。

当接收到用户的呼叫请求时，交换机应首先对用户进行身份认证，如果用户通过身份认证，则先在本地的路由信息表中查询用户的ID，如果被叫方是本地用户，转而询问本地用户状态表看是否处于空闲可用状态。

若被叫方不在本地网中，则通过其他量子交换机来交换路由信息，从而建立正确的路由信息，再由量子交换机向被叫用户发出请求，告知主叫方的ID，等待检查，并在收到应答后分析被叫用户是否已经接入网络，是否空闲且准备好接收消息。

若被叫用户被判定为不可用（如用户线路忙、不存在、链路未准备好、故障等），则由服务器将具体原因告知主叫方；若被叫用户同意接收，交换服务程序先将主叫用户和被叫用户双方都设置为忙，再根据路由信息查询链路资源表核实信道，接口及通信波长，如果符

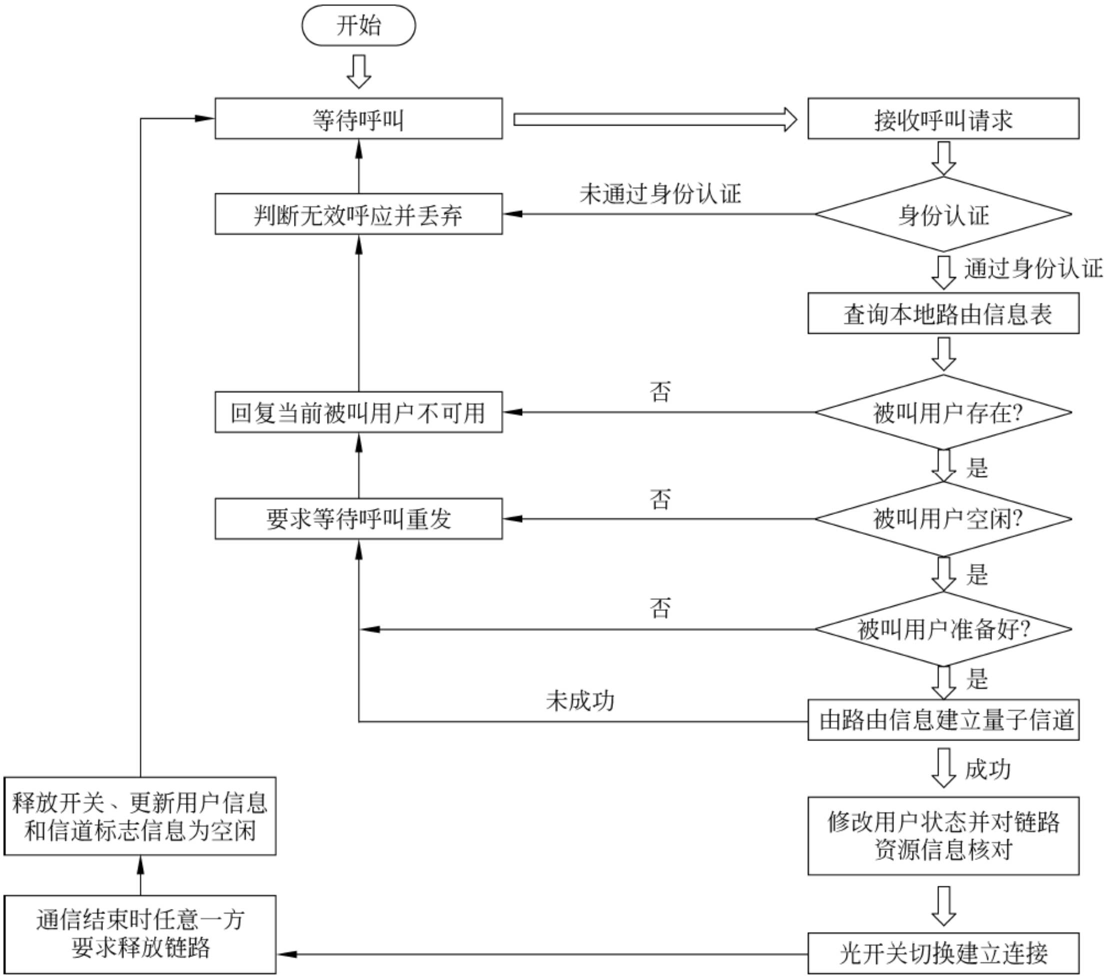

开始
等待呼叫
接收呼叫请求
身份认证
未通过身份认证
判断无效呼应并丢弃
通过身份认证
查询本地路由信息表
被叫用户存在?
否
回复当前被叫用户不可用
是
被叫用户空闲?
否
要求等待呼叫重发
是
被叫用户准备好?
否
是
由路由信息建立量子信道
未成功
成功
修改用户状态并对链路资源信息核对
光开关切换建立连接
通信结束时任意一方要求释放链路
释放开关、更新用户信息和信道标志信息为空闲

图 6-25　量子交换机交换控制流程

合通信条件，再通过修改相应的信道表将对应的信道设置为忙并控制光开关物理连接，给主叫方发送呼叫连接的结果；若被叫用户应答拒绝接收，则交换机直接将通信终止信息反馈给主叫用户。连接控制任务到此结束。

完成操作后修改用户状态标志表和信道状态标志表，将相应的项标记为空闲状态，等待下一次连接。物理链路在双方通信结束之前应维持连接不中断，在通信结束后，由请求方发送释放请求到交换机，交换机接收到释放请求消息后，断开双方链路上的光开关并将当前连接置为空闲，然后将用户状态标志表和信道状态标志表相应的项标记为空闲状态，

等待下一次连接。

由以前的介绍可以得知，使用BB84协议的QKD是无条件安全的，然而此密钥分配协议无法检测出是否有窃听者冒充通信的双方，在传统的量子交换机中，也并没有加入身份认证的模块。因此，为了获得安全的密钥，可以在量子交换机的呼叫连接模块中加入了量子身份认证模块，以带身份认证的BB84协议为例，对各个进行呼叫连接请求的用户进行身份认证。

身份认证是指验证某个用户是否确实是它自己所声称的那个用户。通常使用的方法是输入该用户的个人信息，经某种公式和算法运算，对比所得的结果，是否与从数据库中存储的信息经公式和算法运算所得结果相同。

一个身份认证体系通常由三方组成：其一是出示证件的人，称为示证者（Prover），提出呼叫连接请求；其二是验证者（Verifier），检验示证者提出证件的正确性与合法性，决定是否满足其请求；第三方是窜扰者（Tamper），是伪装成Prover骗取Verifier信任的窃听者，可以窃听合法用户的通信。

量子身份认证是指，根据Prover提供的信息对其身份进行确认，其中示证者提供的信息可以是经典的也可以是量子的。然而，对于实现身份认证的三个主要元素，即示证者的个人信息、信息处理系统以及数据库系统，至少需要有一个是量子的，在这种方式下形成的身份认证系统称为量子身份认证系统。

以通信双方事先共享一个预定好的比特串为例，通过对此比特串的对比来表明自己是合法通信者，即Prover提供的个人信息与数据库系统存储的信息都属于经典信息，这样可以避免需要对量子态进行保存的技术难题。

在信息处理系统中，可以将Prover的个人信息转化为量子信息再进行处理和传输，实现可证明安全的量子身份认证。对于这种带身份认证的BB84协议，约定Alice与Bob事先已经获得一串经典信息比特串kab作为共享认证密钥。

作为认证密钥的kab仅在通信中使用一次，每次认证后都能通过双方分配密钥进行动态更新，从而确保了认证密钥的安全性。带身份认证的BB84协议与原BB84协议的不同点主要在于，需要将随机发送的量子比特串中的某些比特设定为特定的认证密

钥位，量子比特串中每四个比特中有一个是特定的认证密钥位，它的具体位置由认证密钥决定，通过此认证位比特所代表的测量基矢与光量子偏振态来实现通信双方的身份认证，所以，认证位的量子态信息不能随机发送，需要根据特定的规则由双方共享的认证密钥所决定。

6.4.3 世界太大了：量子中继器

量子通信系统使用纠缠光子对作为信号源，而量子中继器通过纠缠制备、纠缠分发、纠缠纯化和纠缠交换来实现中继功能的转换器。量子信号的传输距离由中继级数决定。使用这种中继器的量子通信系统可以用于长距离量子通信。

1. 量子中继器的提出背景

量子通信由于其独特的绝对安全功能，越来越受到各国学者的重视。在长距离量子通信系统中，可以依靠事先建立的、空间分离的两体“理想”纠缠纯态传输信息，它们是量子通信的重要资源。但是，由于量子通信系统与信道的相互作用，会引起系统中纯态的相干性衰减，从而丧失了各叠加成分之间的相对因子的确定性，使各叠加成分的内部相位差的随机性增加。

于是寄托在这种内部相干性上的量子信息就会衰减，这种衰减随着信息传输距离的增加而增加，最终，使得量子信息传输失败。因此，需要在长距离系统中使用量子中继器。

2. 量子中继器的主要功能

一般来说，经典通信中，在利用中继技术恢复信号的能量同时，起了两个方面的作用：一方面恢复了信号的传输特性；另一方面表示信息的比特也随之得到恢复。与经典中继器不同，量子中继器不是一个放大器，需要利用量子态的纠缠与交换来实现量子中继功能。量子中继器的传输过程如图 6-26 所示。

量子通信中的信息载体—量子信号具有量子特性，传输和最终检测的核心部分不是能量而是信号的某种量子状态。研究表明，量子信号的状态同时受到经典噪声和量子噪声的影响，这些噪声会导致量子比特的退相干现象发生，从而导致信息丢失，使得量子通

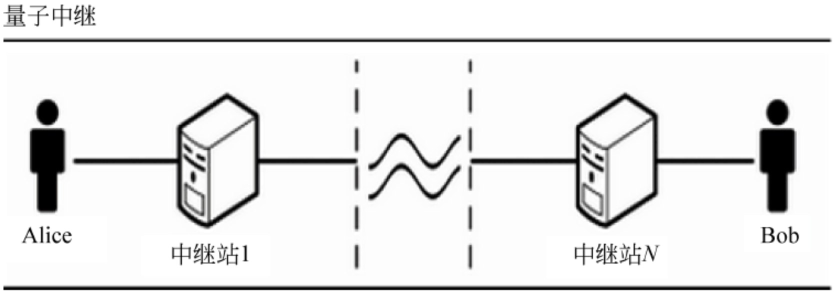


图 6-26　量子中继器

信不能正常进行。另一方面，经典噪声使得量子信号的传输特性不断衰减，导致量子信号不断变弱，最终难以检测。

因此，量子中继应该具有两个方面的功能。

（1）通过补充量子信号的能量实现量子信号的稳定传输。

（2）在补充量子信号能量的同时，保证量子信号携带的量子比特不发生改变量子中继器的工作原理。

对于使用纠缠源的量子通信系统来说，首先借助量子中继技术建立起一个长距离的量子信道，在此基础上，利用所建立的量子信道的量子特性实现安全的量子信号传输。

因此，在这种通信模式中，不会由于量子中继的加入而导致量子通信中信息的丢失。不过，这种通信模式的重要前提条件是，量子中继不会导致量子信道原有特性的改变。例如，若采用量子中继技术，量子通信协议中纠缠光子对的最大纠缠性不能发生改变。

根据上述特征，这种通信模式下的量子中继技术必须发挥两个方面的作用：一是补充信号的能量；二是维持量子信道的原有特性。

大多数物理学家提出的量子中继器方案中含有 CONT 运算，但当前还没有实现能够达到误差不超过百分之几的能用于长距离量子信道的 CONT 运算。

因此，采用只利用线性光学器件的方案，以纠缠光子对作为量子信息的传送通道，采用量子中继器的目的是增加高品质纠缠光子对的作用距离。通过对短程纠缠光子对进行纠缠纯化和纠缠交换，得到高纠缠度的长程纠缠光子对，从而建立起长距离的量子信道。

6.4.4 量子通信产业链

1. 量子通信产业链分析

量子通信产业链上游主要是信号处理芯片、雪崩光电二极管(APD)等元器件及各类核心设备。国内能够提供核心设备的公司并不多,国外厂商主要包括瑞士 IDQ 公司、美国 Bennet 公司等。

量子通信产业链中游主要包括网络传输干线提供商和系统集成商。以量子保密通信“京沪干线”技术验证及应用示范项目为例,提供传输干线服务的公司是中国有线电视网络有线公司,提供系统集成服务的公司包括神州数码系统集成服务有线公司、中国通信建设集团有线公司等。

量子通信产业链下游主要是各种行业应用,如金融、军事、政务、商务等领域。提供的产品包括量子电话、基于量子保密技术的 IDC、量子白板等。量子通信产业链的组成如图 6-27 所示。

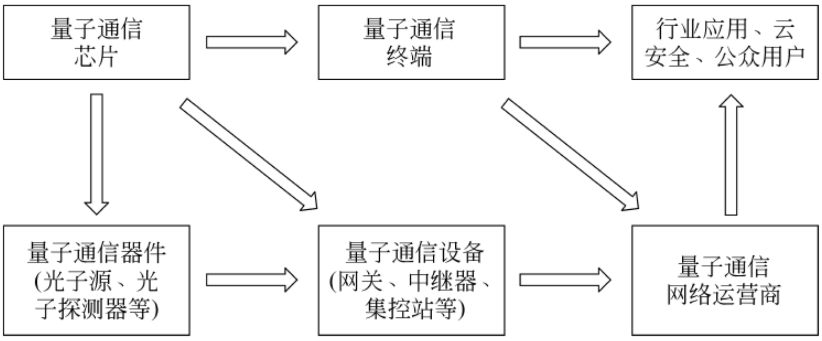

量子通信芯片
量子通信终端
行业应用、云安全、公众用户
量子通信器件(光子源、光子探测器等)
量子通信设备(网关、中继器、集控站等)
量子通信网络运营商

图 6-27　量子通信产业链的组成

2. 量子通信核心设备

量子通信核心设备是量子保密通信产业链中最核心的一个环节。核心设备主要包括量子密钥分发设备、量子交换机、量子安全网关、量子网络站控设备、量子随机数发生器等。

1）量子密钥分发设备

量子密钥分配终端主要负责量子通信过程中密钥的收发。密钥分配终端根据结构的不同，可以分为收发独立型结构和一体型结构。收发独立型设备是指发送端机和接收端机分为两个独立设备，也称为单向量子密码系统。收发一体型设备包含量子密钥发射端和接收端，也称为双向量子密码系统，组网较灵活。

量子密钥分发网络密码机将量子密钥分发技术与传统商用密码技术有效融合，可实现大容量、高性能的网络数据加密传输。相比传统网络安全设备，该产品不仅确保了敏感的密钥分发过程的安全性，而且密钥更新速度更快、业务密钥生命周期更短，从而使系统的安全性得以大幅提升，满足了各种基于网络的应用系统对信息安全的需求。

2）量子交换机

量子交换机用于多个量子密钥分配终端设备间量子信道的搭建，是量子通信网络中实现量子信道共享的设备，位于网络拓扑的汇聚节点，集中管理网络信道资源。光量子交换机按光路切换类型可分为全通型和矩阵型。

全通型量子交换机可以实现所有光端口两两互连，矩阵型光量子交换机可以实现内外光端口互连。

3）量子安全网关

量子安全网关是量子通信组网中的核心设备，是完成量子密钥分发的最基本器件。量子密钥由量子网关通过光纤链路分发。量子网关内部集成有光源、探测器和电子学板卡，能够实现普通电话、传真、IP 电话、视频会议及文件传输等的应用接入，对语音、视频、数据等使用量子密钥进行高安全保密通信。按所处区域不同，量子网关分为可信中继量子网关和普通量子网关。

量子网关主要完成以下功能。

（1）量子密钥分发与管理。

（2）数据加解密：加解密算法可根据业务类型、优先级、密钥类型等进行选择。

（3）应用接入：为普通电话、传真、VoIP 电话、视频会议提供标准接口。

（4）网络接口及其他功能。

4）量子网络站控设备

量子集控站由光量子交换机、量子通信服务器和量子密钥分发终端组成。利用多个量子集控站组成多种网络拓扑，可以提高组网的灵活性和稳定性，能方便地对量子通信网络进行扩展，扩大量子通信网络的覆盖面积，大大扩展通信距离。已建成的“合肥城域量子通信试验示范网”和“济南量子通信试验网”，都是基于量子集控站实现的多用户量子通信网络。

5）量子随机数发生器

量子随机数发生器是基于量子物理和量子效应而产生的真随机数的系统，在实用化量子密码系统等对随机性质量和安全性要求较高的领域具有重要的应用。比特率是量子随机数发生器最重要的指标。早期的量子随机数发生器利用单光子路径选择方案，比特率仅为 4Mbps。

实用化量子通信领域的一个重要目标是将量子密码系统的工作频率提升至 10GHz，需要至少 50Gbps 以上的量子随机数发生器对单光子脉冲进行调制编码。

第7章

量子世界的‘看门狗”——安全及密码

传统的保密通信可以分为加密、接收、解密三个过程，发送者将发送内容通过某种加密规则(密钥)转化为密文，接收者在接到密文后采用与加密密钥匹配的解密密钥对密文进行解密，得到传输内容。

量子保密通信的过程也相同，只不过作为加密和解密的密钥不再是传统的密码，而是改用微观粒子携带的量子态信息。这一看似微小的变化，使密钥的安全性产生了彻底变化。

古人在信封上用火漆封口，一旦信件被中途拆开，就会留下泄密的痕迹。量子密钥在量子通信中的作用比火漆更彻底，一旦有人试图打开信件，量子密钥会让信件自毁，并让使用者知晓。只要量子力学规律成立，量子保密通信就无法被破解。

2400 多年来，密码作为保护信息的手段，在军事、外交、经济、生活等领域得到全方位应用。然而，尽管经历了手工加密、机器编码、计算机编码等不断升级的过程，密码变得越来越复杂、越来越可靠，但迄今无论什么样的高级密码，依然都有被破解的可能。那么，有没有一种绝对不被破译的密码，能让传送的信息安全可靠?

7.1 “看门狗”的祖宗：经典密码学与现代密码学

密码学是一门古老的学科，其历史极为久远，可以追溯到几千年前的古文明时期。古典密码的设计和破解通常凭借灵感和技巧，而不是推理和证明，充满艺术性。密码学也是一门新兴的学科，1949 年香农将信息论引入了密码学，为现代密码学建立了理论基础。

随着 Data Encryption Standard(DES) 密码系统，Rivest-Shamir-Adleman(RSA)公钥密码系统等在军事、商业和民用领域的广泛应用，密码学作为一门学科迸发出巨大的生命力。

1994 年，Shor 在理论上提出一种在量子计算机上运行的算法，可以破解 RSA 公钥密码体系；随着量子力学的发展，基于经典算法的密钥将无密可保！而基于量子力学基本原理，并在理论上是无条件安全的真随机数量子密钥分发的出现，引起了各国科学家极大的兴趣。量子密钥分发(Quantum Key Distribution，QKD)成为量子信息领域中第一个走向实用的技术。

下面对古典密码、现代密码以及量子密钥分发进行介绍。

7.1.1 古罗马人的密信：经典密码学

早在公元前 400 多年，人类已经有意识地利用一些技巧对信息加密。古希腊人发明了用于传递军事机密的密码棒(见图 7-1)，即把长条的皮革螺旋形地斜绕在一个多棱棒上；将情报内容沿棒的径向方向写下。解下皮革后，文字乱杂无规，这就是密文，对敌人毫无价值。而接收消息的友方有一根同样尺寸的棒子，将皮革绕到棒子上，情报即会显现。

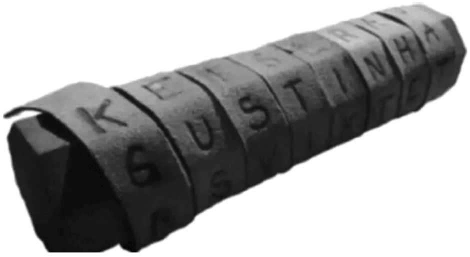


图 7-1 古希腊密码棒

这种密码技术有如下特点。

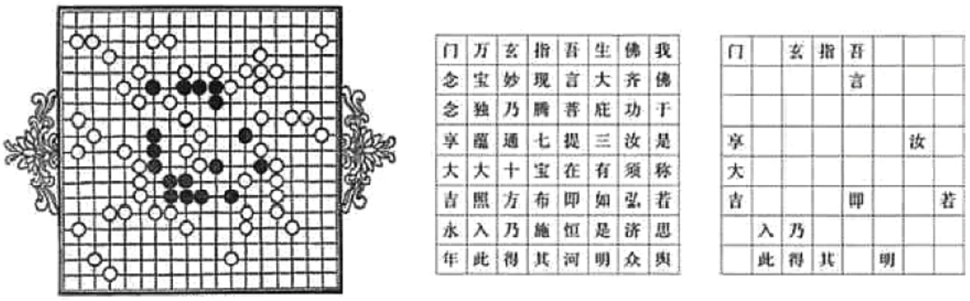
(1) 加密和解密的方法难度一致。

(2) 知道加密的方法即知道解密的方法。

(3) 加密方法除敌方外，对第三者也是保密的，所以第三者无法对友方发送加密信息。

我国古代也早有将“密语”隐藏在诗文、画卷或棋盘中特定位置的记载。在荷兰汉学家高罗佩所著的中国公案小说《大唐狄公案》中，有描述狄仁杰解开层层通关密码破获一出谋反案的“湖滨案”。

故事讲述一个歌女被害，留下的线索是一张棋谱残局，狄公百思不得其解。在继续追查的过程中，得到了另外一个线索，一幅金牒玉版的经文。种种推断失败后，狄公灵机一动，将棋谱中的黑子与经文进行对比，显现信息：“若汝明吾言，即指其玄，乃得入此门，享大吉。”然后凭此打开密室门，找到谋反的军火库，破获大案。湖滨案中的密码、明文以及解密后的信息（摘自《大唐狄公案》）如图 7-2 所示。



(a) 残局(密码)

门	万	玄	指	吾	生	佛	我
念	宝	妙	现	言	大	齐	佛
念	独	乃	腾	菩	庇	功	于
享	蕴	通	七	提	三	汝	是
大	大	十	宝	在	有	须	称
吉	照	方	布	即	如	弘	若
永	入	乃	施	恒	是	济	思
年	此	得	其	河	明	众	舆

(b) 金牒玉版(明文)

门		玄	指	吾			
				言			
享						汝	
大							
吉				即			若
	入	乃					
	此	得	其		明		

(c) 信息

图 7-2　“湖滨案”中的密码、明文以及解密后的信息（摘自《大唐狄公案》）

在此案中，棋盘残局是密码，本身无特点；金牒玉版的经文对应明文，是加密过的信息，也要求无敏感词。

7.1.2　德国人第二次世界大战时使用的密码机：现代密码学

第二次世界大战时德国军方使用的“恩尼格码”机使密码的编制进入新的现代密码学阶段。

恩尼格码机内置了多个转子，每个转子对应不同的 26 个字母，也就是说，只要发送者敲下一个字母就会出现 26^N 种可能，而其中规律只有德国军方自己才知道，如果盟军截获了信息，靠人工推演，可能要花费上万年才能破译。恩尼格码机如图 7-3 所示。

图 7-3　恩尼格码机

1. 现代密码学

现代密码学是一门快速发展的学科，现有的密码体制可以分为单钥密码（对称密码体制，如 DES 密码）和公钥密码（非对称加密体制，如 RSA 密码）。前者使用相同的密钥，并且加密、解密过程一致；后者使用不同的公钥和私钥。下面主要介绍广泛应用于网络、电子银行系统等领域的 RSA 公钥密码系统。

1976 年 Diffie 和 Hellman 在《密码新方向》中提出了著名的 Diffie-Hellman 密钥交换协议，标志着公钥密码体制的出现。1978 年，Rivest、Shamir 和 Adleman 实现了 RSA 公钥密码体制。

RSA 密码系统的工作原理

RSA 算法基于简单的数论事实：将两个大的质数相乘十分容易，但是想要对其乘积进行因式分解却极其困难。在 RSA 密码体制中，加密协议和解密协议（算法）是公开的。加密密钥是公开信息，即公钥（public key），而解密密钥是需要保密的，即私钥（private key）。公钥决定私钥，但无法根据公钥计算出私钥。这样的密码体制，使任何人（第三者）都可以给私钥拥有者传送经过公钥加密过的信息（多对一），但是经过加密的信息第三者很难破解。

RSA 算法的核心问题是产生公钥、私钥的密钥对，其中，(N,c)是公钥，(N,d)是私钥（除 N 和 c 外，其他数都不能公开）。利用生成的密钥对，甲方将需要传送的信息 X（明文）经公钥加密，变成密文 Y，传送给乙方；乙方利用私钥解密，得到甲方传送的信息（见

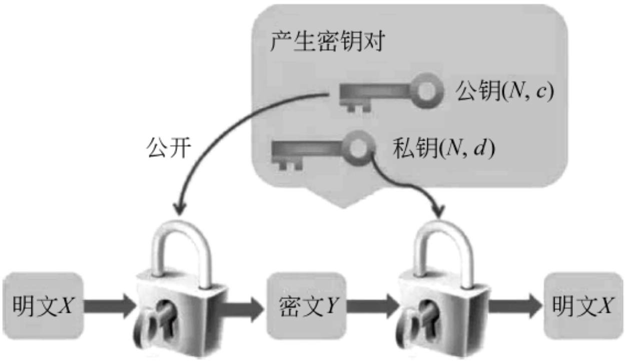


图 7-4　RSA 公钥密码系统的工作原理

图 7-4）。

2. RSA密码系统现状

RSA 算法广泛应用于数据加密和数字签名，当前商业、民用等领域一般使用 1024 位的密钥。攻击 RSA 算法最普遍的方式是分解模数 N，基于大数分解极其困难，RSA 目前能够抵抗已知的绝大多数密码攻击，已被国际标准化组织（ISO）推荐为公钥数据加密标准。

历史上，曾对破解 RSA 密码有过一次悬赏。1977 年，Gardner 用 RSA 方法设计了一段密码，并公开悬赏 100 美元。他将一个英文句子转换为明文的字符串（对应方式：将 26 个英文字母用 01～26 表示，空格用 00 表示），将这个字符串用公钥（N，c）加密，其中，模数 N 是一个 129 位的十进制数（RSA-129），$c=9007$。密码破解的关键是将模数 RSA-129 因式分解。

1995 年，互联网上 1600 台工作站大约用了 8 个月的时间，估计微处理器 5000 MIPS 年（MIPS 指每秒百万指令），终于破解了这个密码，并获得隐藏的神秘信息：The Magic Words are Squeamish Ossifrage（咒语是易恶心的秃鹫）。随着处理器能力的提高，RSA-130、RSA-140 相继被分解；到 1999 年，RSA-155（512 位）被成功分解，用时 5 个月（约 8000 MIPS 年）。

假设计算机处理能力遵循摩尔定律，即每 18 个月翻一番，考虑 1000 台工作站联合计

算分解 RSA 模数。以 RSA-155 的破解时间做参考，在 2000 年，计算机处理能力约为 800 MIPS，则 1000 台处理器同时计算，需要 4 天破解。可以估算出模数 N 分别为 1024 位、2048 位、4096 位时在不同年限下需要的分解时间，结果如图 7-5 所示。其中，横轴表示年份，纵轴表示分解需要的时间(以年为单位)。从图 7-5 中我们可以看出，目前广泛应用的 1024 bits 密钥长度是安全的。

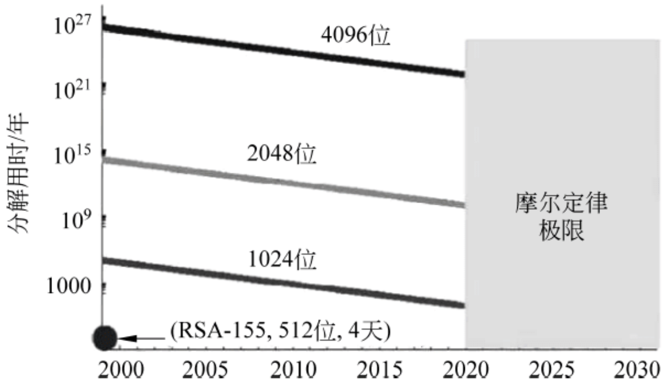


图 7-5　RSA 不同位数公钥密码随年份被分解时间展示

可以总结得到，RSA 密码系统的安全性建立在 N 很难分解的基础上，或者说利用已知的算法 N 很难分解；破解 RSA 密码系统，需要很大的计算资源。所以，在考虑采取的 RSA 密码时，只需考虑在现有计算能力基础上，需要一个较长时间(比如 10 年)才能破解，就可以被认为是安全的。因此，RSA 密码系统的安全性是一个动态的过程。

3. RSA 密码系统的未来——量子计算机将使基于算法的密钥无密可保

对于因子分解，经典算法的计算量随位数的变化是指数增长。1994 年 Shor 宣布了量子算法求质因子方法，计算量随位数的变化是多项式增长，计算速度指数地快于经典算法。Shor 算法的数学原理依赖于计算取 N 模时 $X_2=1$ 有除正负 1 之外的非平庸解，并从而实现因子分解 N，其优势依赖于可快速实现的量子傅里叶变换。

假设有一台频率为 100 MHz 的可以运行此算法的量子计算机，分解时间随整数 N 位数的变化情况如图 7-6 所示。其中，横轴表示被分解整数的二进制位数，纵轴表示分解需要的时间(以分钟为单位)。Shor 算法展示了量子计算机上可以有效解决因子分解问

题，一个足够大的量子计算机可以破解RSA公钥密码系统。这鼓励科学家去建立量子计算机和研究新的量子计算机算法。

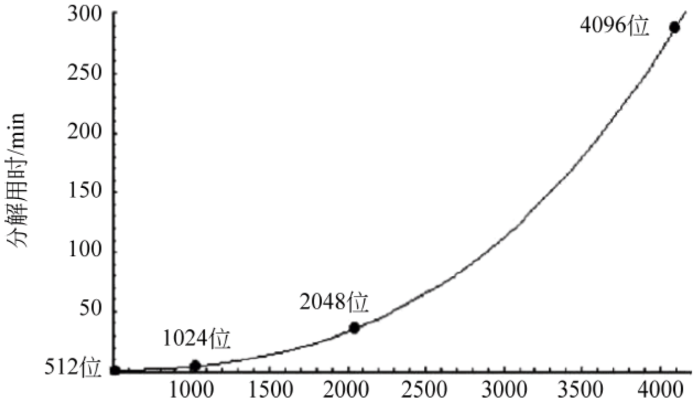


图7-6　利用100 MHz量子计算机分解二进制整数需要的时间

2001年，IBM公司的一个小组利用核磁共振资源，在实验上实现了Shor的量子分解算法，将15分解成3×5。2012年，中国科学技术大学微尺度国家实验室的杜江峰等人利用核磁共振系统成功地在实验上实现了143＝11×13的量子分解。目前，D-Wave公司也已建成千量级量子比特的特定结构量子计算机——量子退火机。可以展望，随着量子计算机的实际应用，届时，基于算法的密钥系统将无密可保！

4. 一次一密密码本

量子计算机如果研制成功，目前广泛应用的经典密码系统将彻底失效，那世界上没有安全的密码了吗？

科学家们想到了已经从数学上严格证明了“一次一密”的密码本是绝对安全的。一次一密要求：密钥完全随机，密钥长度和明文长度一样长，密钥本身只使用一次。这使分配密钥成为十分重要的环节，然而现实中存在以下问题。

(1) 发射方Alice和接收方Bob之间的密码本需要传递，才能异地共享。

(2) 密码本在传送信息之前就存在，时间上靠前。

(3) Alice和Bob即使有身份认证，不能防止敌对方也有一个相同的密码本，即对泄密无感知。

量子力学对安全通信关上一扇窗的同时，也打开了一扇门。科学家发现，利用量子力学的基本原理，既可以轻松实现一次一密，又能保证密钥分发过程绝对安全，是原理上无条件安全的保密通信。

7.2 量子密码的鼻祖：海森伯测不准原理

图 7-7　海森伯

海森伯(见图 7-7)是德国著名物理学家，量子力学的主要创始人，哥本哈根学派的代表人物，1932 年诺贝尔物理学奖获得者。他的《量子论的物理学基础》是量子力学领域的一部经典著作。鉴于他的重要影响，在美国学者麦克·哈特所著的《影响人类历史进程的 100 名人排行榜》，海森伯名列第 43 位。

不确定性原理是由海森伯于 1927 年提出，这个理论是说，你不可能同时知道一个粒子的位置和它的速度，粒子位置的不确定性表明微观世界的粒子行为与宏观物质很不一样。

7.2.1　海森伯不确定原理

不确定性原理又称为“测不准原理”“不确定关系”，是量子力学的一个基本原理。德国物理学家海森伯于 1927 年发表论文，给出该原理的原本启发式论述，因此该原理又称为“海森伯不确定性原理”。

为什么会测不准?

在量子力学里，不确定性原理表明，粒子的位置与动量不可同时被确定，一个微观粒子的某些物理量，不可能同时具有确定的数值，其中一个量越确定，另一个量的不确定程度就越大。类似的不确定性关系式也存在于能量和时间、角动量和角度等物理量之间。

根据不确定性原理，如果要预测一个粒子在未来某时刻的位置与速度，人们必须要精准地测量出它现在的位置和速度。但是，人们无法将粒子的位置精确到比光波两个波峰

之间的长度更短。

根据普朗克的量子假设，至少需要用到一个光量子。然而这个量子就会对粒子产生扰动，并且将以一种无法预见的方式改变粒子的速度。位置测量越准确，所需要的波长越短，单个量子的能量越大，这样一来，粒子的速度也将被扰动得更加厉害。

这项原理陈述了精确确定一个粒子，例如原子周围的电子的位置和动量是有限制的。这个不确定性来自两个因素，首先测量某东西的行为将会不可避免地扰乱那个事物，从而改变它的状态；其次，因为量子世界不是具体的，但基于概率，精确确定一个粒子状态存在更深刻、更根本的限制。

海森伯测不准原理是通过一些实验来论证的。设想用一个 γ 射线显微镜来观察一个电子的坐标，因为 γ 射线显微镜的分辨本领受到波长 λ 的限制，所用光的波长 λ 越短，显微镜的分辨率越高，从而测定电子坐标不确定的程度就越小。但另一方面，光照射到电子，可以看成是光量子和电子的碰撞，波长 λ 越短，光量子的动量就越大。

再如，用将光照到一个粒子上的方式来测量一个粒子的位置和速度，一部分光波被此粒子散射开来，由此指明其位置。但人们不可能将粒子的位置确定到比光的两个波峰之间的距离更小的程度，所以为了精确测定粒子的位置，必须用短波长的光。

但普朗克的量子假设，人们不能用任意小量的光：人们至少要用一个光量子。该量子会扰动粒子，并以一种不能预见的方式改变粒子的速度。

所以，简单来说，就是如果要想测定一个量子的精确位置，那么就需要用波长尽量短的波，这样的话，对这个量子的扰动也会越大，对它的速度测量也会越不精确；如果想要精确测量一个量子的速度，那就要用波长较长的波，那就不能精确测定它的位置。

为了方便理解，举一个经典物理中的例子对不确定原理进行说明：经典物理中波的频率与波的到达时间之间就存在着不确定性，如果想要测量频率，就需要等几个波峰到达，这样一来，便无法精确地测量出波的到达时间了。

由海森伯不确定原理可知，对于任何一个物理量的测量都将不可避免地对测量另一个物理量产生干扰。所以，这个原理也是保证通信双方能够检测到信息是否被窃听的基础，是保证通信双方无须事先交换密钥即可进行绝密通信的关键。

7.2.2 测不准原理所起的作用

测不准原理所起的作用在于它说明了科学度量的能力在理论上存在的某些局限性，具有巨大的意义。

如果一个科学家用物理学的基本定律甚至在最理想的情况下也不能获得有关他正在研究的体系的准确知识，那么就显然表明该体系的将来行为是不能完全预测出来的。根据测不准原理，不管对测量仪器做出何种改进都不可能会使人们克服这个困难。

不确定性原理表明从本质上来讲物理学不能做出超越统计学范围的预测（例如，一位研究放射的科学家可能会预测出在三兆个原子中将会有两百万个在翌日放射 γ 射线，但是他却无法预测出任何一个具体的镭原子将会是如此）。在许多实际情况中，这并不构成一种严重的限制。

在牵涉巨大数目的情况下，统计方法经常可以为行动提供十分可靠的依据；但是在牵涉到小数目的情况下，统计预测就确实靠不住了。

在微观体系里，测不准原理迫使人们不得不抛弃严格的物质因果观念。这就表明了科学基本观发生了非常深刻的变化；的确是非常深刻的变化，以至于像爱因斯坦这样一位伟大的科学家都不愿意接受。爱因斯坦曾经说过：“我不相信上帝在和宇宙投骰子。”然而这却基本上是大多数现代物理学家感到必须得采纳的观点。

显而易见，从某种理论观点来看，量子学说改变了人们对物质世界的基本观念，其改变的程度也许甚至比相对论还要大。然而量子学说带来的结果并不仅仅是人生观的变化。

在量子学说的实际应用的行列之中，有诸如电子显微镜、激光器和半导体等现代仪器。它在核物理学和原子能领域里也有许许多多的应用；它构成了人们的光谱学知识的基础，广泛地用于天文学和化学领域；它还用于对各种不同论题的理论研究，诸如液态氦的特性、星体的内部构造、铁磁性和放射性等。

7.3　我的地盘我做主：量子密码学

随着计算机网络技术的持续、快速发展，网络通信、电子商务、电子政务、电子金融等应用使人们越来越多地依赖网络进行工作和生活，大量敏感信息需要通过网络传输，人们需要对自己的信息进行保护以免被窃取或篡改，密码学为我们提供了有力的保证。

随着密码学的发展，量子密码开始走入人们的视线。量子密码是以现代密码学和量子力学为基础、量子物理学方法实现密码思想和操作的一种新型密码体制。这种加密方法是用量子状态来作为信息加密和解密的密钥。量子的一些神奇性质是量子密码安全性的根本保证。

与当前普遍使用的以数学为基础的密码体制不同，量子密码以量子物理原理为基础，利用量子信号实现。与数学密码相比，量子密码方案具有可证明安全性（甚至无条件安全性）和对扰动的可检测性两大主要优势，这些特点决定了量子密码具有良好的应用前景。随着量子通信以及量子计算的逐渐丰富与成熟，量子密码在未来信息保护技术领域将发挥重要作用。

量子密码是采用量子力学原理，通过公开的信道在异地用户之间能严格保证分配过程安全的密钥分配方法，可以说，量子密码＝量子密钥分配。

量子密码的本质是用于解决分配问题的私钥体系，其意义在于：它是解决现有密码体系的本质问题的一种新的密码学方法。

量子密钥分配的安全保证主要如下。

（1）以单光子（量子）携带信息，不怕别人获取信息。

（2）量子不可克隆定律保证别人不可能复制信息。

7.3.1　量子密码的起源与发展

1. 量子密码的起源

最早想到将量子物理用于密码术的是美国科学家威斯纳。他于1970年提出，可利用单量子态制造不可伪造的“电子钞票”。但这个设想的实现需要长时间保存单量子态，不

太现实，并没有被人们接受，但他的研究成果开创了量子密码的先河，在密码学历史上具有划时代的意义。

直到1984年贝内特和布拉萨德提出著名的量子密钥分配协议，也称为BB84方案，由此迎来了量子密码术的新时期。5年后，他们在实验室里进行了第一次实验，成功地把一系列光子从一台计算机传送到相距32cm的另一台计算机，实现了世界上最安全的密钥传送。

1992年，贝内特又提出一种更简单但效率减半的方案，即B92方案。经过30多年的研究，量子密码以及发展成为密码学的一个重要分支。

2. 量子密码的基本特征

密码学之所以能够被人们接纳，并成为受到密码学界、物理学界、商家、媒体、政府部门等各方面广为关注的密码学分支和保护信息的重要技术手段之一，主要原因在于量子密码本身的独特属性。使得量子密码相比数学密码更具应用上的优势，体现在以下两个方面：对信道中窃听行为的可检测性和方案的高安全性(可证明安全性或者无条件安全性)。

密码方案的无条件安全性是指量子密码方案在攻击者具有无限计算资源的条件下仍不可能破译该密码方案的特性。无条件安全性又称为信息安全，其基础是信息理论。

对信道中窃听行为的可检测性是指通信中的两个用户之间的信道受到干扰时，通信者根据某个量子力学原理可以同步实时地检测出这种干扰的存在与否。对信道中窃听行为的可检测性特征没有经典对应，是一种独特的量子效应，这种特性是保证量子密码方案具有高安全性的重要基础之一。这些特征使得量子密码在信息保护通信方面具有良好的优势。

3. 量子密码研究进展

近年来，研究者们设计出了大量的各具特色的量子密码方案，并对其安全性进行了深入系统的分析，同时在提高方案性能和实验实现方面取得众多成果。

7.3.2 量子密码技术的原理

1. 量子密码技术的原理介绍

从数学角度讲，只要掌握了恰当的方法，任何密码都可破译。此外，由于密码在被窃

听、破解时不会留下任何痕迹，用户无法察觉，就会继续使用同地址、密码来存储传输重要信息，从而造成更大损失。然而量子理论将会完全改变这一切。

自20世纪90年代以来，科学家开始了量子密码的研究。因为采用量子密码技术加密的数据不可破译，一旦有人非法获取这些信息，使用者就会立即知道并采取措施。无论多么聪明的窃听者在破译密码时都会留下痕迹。更惊叹的是量子密码甚至能在被窃听的同时自动改变。毫无疑问，这是一种真正安全、不可窃听破译的密码。

以往密码学的理论基础是数学，而量子密码学的理论基础是量子力学，利用物理学原理来保护信息。其原理是海森伯测不准原理中所包含的一个特性，即当有人对量子系统进行偷窥时，同时也会破坏这个系统。因此，对输运光子线路的窃听会破坏原通信线路之间的相互关系，通信会被中断，这实际上就是一种不同于传统需要加密解密的加密技术。

在传统加密交换中两个通信对象必须事先拥有共同信息——密钥，包含需要加密、解密的算法数据信息。而先于信息传输的密钥交换正是传统加密协议的弱点。另外，还有“单量子不可复制定理”。它是上述原理的推论，指在不知道量子状态的情况下复制单个量子是不可能的，因为要复制单个量子就必须先做测量，而测量必然会改变量子状态。根据这两个原理，即使量子密码不幸被计算机黑客获取，也会因测量过程中对量子状态的改变使得黑客只能得到一些毫无意义的数据。

量子密码就是利用量子状态作为信息加密、解密的密钥，其原理是量子纠缠。它是一种量子力学现象，指不论两个粒子间距离有多远，一个粒子的变化都会影响另一个粒子。因此，当使用一个特殊晶体将一个光子割裂成一对纠缠的光子后，即使相距遥远它们也是相互连接的。只要测量出其中一个被纠缠光子的属性，就容易推断出其他光子的属性。

2.量子密码实现方案

到目前为止，主要有三大类量子密码实现方案。

(1) 基于单光子量子信道中海森伯测不准原理的。

(2) 基于量子相关信道中贝尔原理的。

(3) 基于两个非正交量子态性质的。

量子密码是利用质子的极化方式编排密码。质子能以四种方式极化；水平的和垂直

的，而且互为一组，两条对角线的也是互为一组。要在两端传递量子密钥，其中一种方法就是以激光发出单一光子，光子会以两种模式中的其中一种偏振。光子的第一种偏振方向是垂直或平行（直线模式）；第二种则是与垂直呈45°角（对角模式）。

不管是哪一种模式，光子的不同指向分别代表0或1这两个数字。依惯例，密码学者通常称发送者为Alice，她随机地以直线或对角模式送出光子，发射出一串量子比特。至于接收者则称为Bob，他也随机决定以两种模式之一来测量射入的光子。根据海森伯的测不准原理，他只能以一种模式来测量量子比特，而不能用两种。发送者Alice向接收者Bob发送量子比特如图7-8所示。

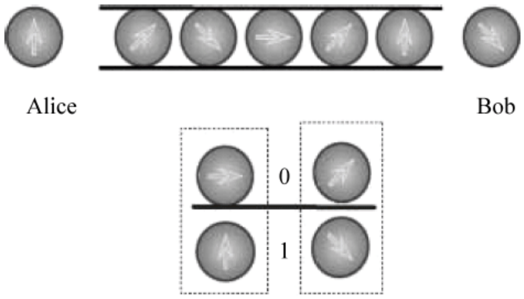


图7-8　发送者Alice向接收者Bob发送量子比特

如果Bob所使用的测量方法与Alice相同，那么他会得到Alice所送的值；如果Bob所使用的测量方法与Alice的不同，所得到的值就不一定和Alice的相同，应该舍弃该位，重新再做，整个步骤如下（传送步骤见图7-9）。

（1）Alice随机选择一个偏振态光子传出。

（2）Bob随机选择一组偏振基同步测量。

（3）Bob实际测得的偏振光子（只Bob知道）。

（4）Bob通知Alice测量到光子用的偏振基（不是态）。

（5）Alice告诉Bob哪些选择是正确的。

（6）双方按约定转换成0、1（如图7-9中，线框圈定的1和0的偏振方向）。

重复上述步骤多次，可以得到一个n位的共同密钥K，用于对信息加密或解密。

因此，量子密钥分配的方案主要如下。

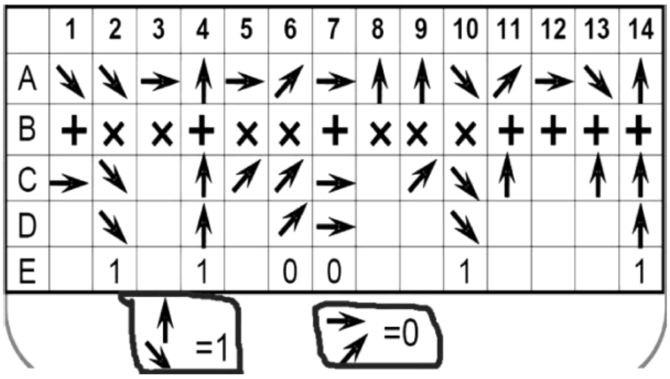


图 7-9　传送步骤

（1）BB84(B92)方案。

（2）EPR 方案。

（3）正交态方案。

（4）信道加密方案。

上述方案是 BB84 方案中按偏振编码的方法，其中光子偏振态代表 0、1，两组（基）共四个不同的偏振态。例如，水平、垂直偏振基，正 45°、负 45°偏振基，Alice 随机选送四个态中的任意一个，Bob 随机选任意一组基测量。该方案的主要优点是简单、易行，适用于自由空间密钥分配。

如果窃听者（称为 Eve）想拦截这道光子流，由于海森伯原理的关系，她无法两种模式都测。如果她以错误的模式进行测量，即使她将该位依照测到的结果重传给 Bob，都一定会有 1/2 机会出错。

Alice 和 Bob 可以随机选择一些位进行比较，如果比较值有误，就可以知道 Eve 进行了拦截，从而舍弃这次的密钥，再建立新的密钥；如果比较值一致，则可以认为密钥是安全的，舍弃这些用于比较的位后，密钥就可以用于以后信息的加密了。

另外一种方法是，Bob 先准备一对光子，或者是一对在纠缠态中共同地半自转的粒子，然后存储其中一个粒子，并将另外一个传送至 Alice。Alice 在收到的粒子上执行了其中一个特别的操作（操作 1 对半自转的粒子不做任何动作；操作 2 沿着 x、y 或 z 以 180°做自旋，对光子来说，做与偏极值一致的旋转）。这些操作，虽然只对其中一个粒子执行，却

会影响两个联合粒子的量子状态(分开测量这两个粒子并不能够证实)。

Alice传回粒子给Bob,Bob可以共同测量传回的粒子和存储的粒子,从而判定Alice使用了四种操作中的哪一种操作,也即代表了两比特数据的0、1组合。如此一来,这个技术有效地加倍了信息频道的最高容量。

在这个通信之间的窃听者Eve将必须侦测粒子以读取信号,然后依序传送这些信号使她不被发现到,然而这个侦测其中一个粒子的动作将会破坏另外一个粒子的量子关联性,如此一来,两方都可以证实到是否有窃听者的存在。

3. 量子攻击

攻击一个量子密码系统主要有两类方法:经典方法和量子方法。量子攻击方法可分为非相干攻击方法和相干攻击方法。非相干攻击就是攻击者独立地给每一个截获到的量子态设置一个探测器,然后测量每一个探测器中的粒子,从而获取信息。

相干攻击是指攻击者可通过某种方法使多个粒子比特关联,从而可相干地测量或处理这些粒子比特,进而获取信息。有些经典密码分析方法和策略不但可以在经典密码分析中发挥作用,在量子密码分析中也将起到重要的作用。在某些情况下,经典攻击甚至是一种重要的攻击方式。

下面简单介绍几种经典型的量子攻击方法,它们对量子攻击的分析具有较高的参考价值。

1) 截获—测量—重发攻击

截获—测量—重发攻击,即窃听者截获信道中传输的量子比特并进行测量,然后发送适当的量子态给合法接收者,这是最简单的攻击方法之一。

2) 假信号攻击

假信号攻击泛指用自己的量子比特替换合法粒子(或光子),以期利用自己与接收者之间的纠缠来协助达到窃听者的攻击方法。同时,替换以后往往需要辅以其他手段来达到目的。因此,假信号攻击具有多样性,分析起来也相对复杂。

3) 纠缠附加粒子攻击

窃听者在截获信道中的量子比特后,通过幺正操作将自己的附加粒子与合法粒子纠

缠起来，然后将合法粒子重新发给接收者，以期利用这种纠缠获取信息。这就是纠缠附加粒子攻击，通常包括截获—纠缠—重发—测量（附加粒子）四个步骤。这种分析方法在证明协议的安全性时也经常用到。

4）特洛伊木马攻击

特洛伊木马攻击是另外一种由于实现设备的不完美而存在的攻击方法。在这种攻击中，窃听者可以向通信信道中发送光脉冲，并分析它们用户设备反射回来的光信号以试图得到设备信息。一般来说，这种针对实验设备的不完美性来实施攻击的问题通常可以用某些技术手段来解决。

4. 结论

量子密码术是近年来国际学术界的一个前沿研究热点。面对未来具有超级计算能力的量子计算机，现行基于解自然对数及因子分解困难度的加密系统、数字签章及密码协议都将变得不安全，而量子密码术则可达到经典密码学所无法达到的两个最终目的：一是合法的通信双方可察觉潜在的窃听者并采取相应的措施；二是使窃听者无法破解量子密码，无论企图破解者有多么强大的计算能力。

可以说，量子密码是保障未来网络通信安全的一种重要的技术。随着对量子密码体制研究的进一步深入，越来越多的方案被提出来，近年来无论在理论上还是在实验上都在不断取得重要突破，相信不久的将来，量子密码将会在网络通信上得到广泛的应用，人们即将进入到一个量子信息时代。

7.4　Alice和Bob的对话：量子密钥分发

经典保密通信通常分为对称密码系统与非对称密码系统两大类。其中，对称密码系统也称为私钥密码系统，它是让相互通信的两者之间共享一组私钥，发送端利用这组私钥，对所要传递信息进行加密，而接收端则用该私钥对收到的信息进行解密。

对于非对称密码系统，首先由接收端生成一对仅自己知道的密钥，并将其中的一把作为公用密钥向其他方公开；之后得到该公用密钥的发送端，使用该密钥对机密信息进行加

密后再发送给接收端；最后，收端再用自己保存的另一把专用密钥对加密后的信息进行解密。可见只有同时拥有公开密钥与专用密钥的接收方才能对信息进行解密，从而保证了机密信息的安全性，所以，非对称密码系统也称为公钥密码系统。

对于对称密码系统，虽然它的加密与解密的速度都很快，但是其面对首要问题在于，如何保证密钥传输的安全性，即在发送方把密钥交给接收方的过程中，很容易被第三方窃听，引发安全漏洞；另外，如果有 n 个人两两之间进行通信，则需要的密钥数量为 $n(n-1)$，这使得密钥的分发变得十分复杂；而对于非对称密码系统，由于其安全性主要依赖于计算的复杂度，所以它也会面临加解密速度慢、密钥尺寸大的问题。

在各类量子通信系统中，光量子由于其独有的优势，如易传输、易制备、不容易和周围环境相互作用，从而可以快速地利用线性光学元件实现偏振或者路径模式等操作，并且具有较高的保真度，使其成为量子信息的最佳载体。另外，由于经典光通信中比较成熟的实验手段以及光学器件，也都可以应用于以光子作为量子信息载体的实验系统中，所以当前许多量子通信的研究和实验主要是针对光量子进行的。

7.4.1 量子密钥分发

量子信息中的一些概念，如量子密码、量子保密通信等，会让公众产生是用量子的方法直接进行通信的误解。实际上，只是用量子力学原理保证安全地把一个真随机数密钥本分配给通信的双方，用于以后进行加密和解密。密文的发送仍然通过经典的通信手段来完成（见图 7-10）。因此，可以使用更确切的说法“量子密钥分发”。

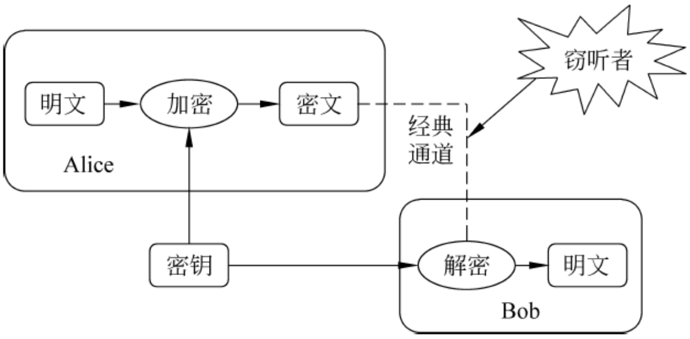


图 7-10　密码通信的基本原理图

7.4.2　BB84 量子密钥分发协议及其工作原理

1984 年，Bennett 和 Brassard 受到 Wiesner 量子钞票概念的启发，提出一种产生密钥的方法，后称为 Bennett-Brassard（BB84）协议，从此 QKD 理论诞生了。

协议被叫作 BB84 算是学术界的传统，因为两位作者的姓氏首字母都是 B，论文正式发表在 1984 年的“international conference on computers, systems and signal processing”会议上。

BB84 需要两条信道，一条量子信道（quantum bit channel）和一条经典信道（classical bit channel）。也就是说，使用 BB84 时，必须保留对经典信道的使用，否则无法完成密钥协商。BB84 协议需要两条信道进行传输示意图见图 7-11 所示。

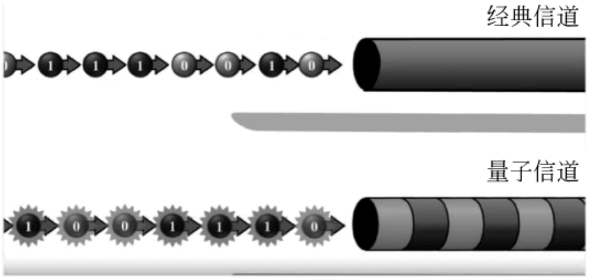


图 7-11　BB84 需要两条信道

协议的运行流程总结如下。

（1）Alice 和 Bob 共享两个极化基（photon polarization bases）D 和 R。

D 和 R 可以被理解为两台“机器”，它们都能各自生成和测量对应 0、1 的量子比特（quantum bit，qbit），如图 7-12 所示。

另一个关键就是，如果将 D 生成量子比特给 R 进行测量，测量结果不可预测。也就是说，如果用 R 来测量由 D 生成的量子比特，测量结果的意义就和直接猜差不多。

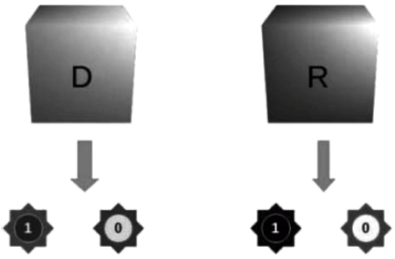


图 7-12　协议的运行流程

接下来开始进行密钥协商，通信首先是在量子信道上进行。

(2) Alice 选出一个 0、1 串 S(如 010001001…011)。

(3) Alice 逐位随机选取 D 或 R，然后通过量子信道发送 S 里 0、1 对应生成的量子态。

(4) Bob 通过量子信道收到 Alice 发送的信息后，随机使用两个极化基 D 和 R 来一位一位地测量量子态，逐个得到 0 和 1。

其后的步骤(4)～(7)都是在今天使用的经典通信信道上进行，而公共信道就代表，如果此时没有别的保护，攻击者完全可以窃听并修改会话内容。

(5) Bob 通过公共信道向 Alice 发送部分自己的测量步骤，即告诉 Alice 自己在每个量子比特上用的到底是 D 还是 R 来做测量。

(6) Alice 对比自己的选择和 Bob 的选择，然后告诉 Bob 他在哪些位置上用的 D 和 R 是正确的。

这些正确位置在 S(即 Alice 先选择的串中)唯一确定了另一个 0、1 比特串，不妨称之为 pms，即类似 TLS 的 pre-master secret。

(7) Bob 收到 Alice 的回应后，随机选择若干个他在正确位上的测量结果告知 Alice。

(8) Alice 确认 Bob 的正确性。如果 Bob 出错，则回到(1)或者终止通信；否则 Alice 给 Bob 发确认信息，同时从 pms 串中剔除 Bob 公布的部分，剩下的作为通信密钥。

(9) Bob 收到 Alice 的确认信息后，同样从 pms 中剔除 Bob 公布的部分，剩下的作为通信密钥。

BB84 的安全性同时依赖于两条信道的安全性。

经由量子信道传输的信息，由于量子态的不可复制和不可存储，且中间人无法知道 Alice 到底用的是 D 还是 R，所以此时，量子信道上信息的保密性是没有问题的。

量子密码用量子比特替代经典比特。经典比特只有 0 和 1 两种状态，根据量子态叠加原理，量子比特既可以处于 0、1 两种状态，也可以处于 0、1 的叠加态上，例如，电子自旋态、光子偏振态等。

假设用单光子的偏振态表示量子比特。一个单光子可以用两种编码方式。

（1）水平和垂直两种偏振态。

（2）45°斜向上和－45°斜向下偏振态。利用码元0对应水平或斜向下－45°的光子偏振方向；而码元1对应垂直或斜向上45°的偏振方向。这样共有4种偏振态，两种编码方式对应于两组互为共轭的测量基(见图7-13(a))。

Alice发射一系列偏振态给Bob，Bob随机选择水平垂直或正负斜向两个共轭基之一的检偏器测量光子的偏振方向。如果测量基与Alice用的发射基一样，则能精确地测定原偏振方向；如果测量基选错了，偏振信息则完全不确定，只有50％的概率会是正确的(见图7-13(b))。

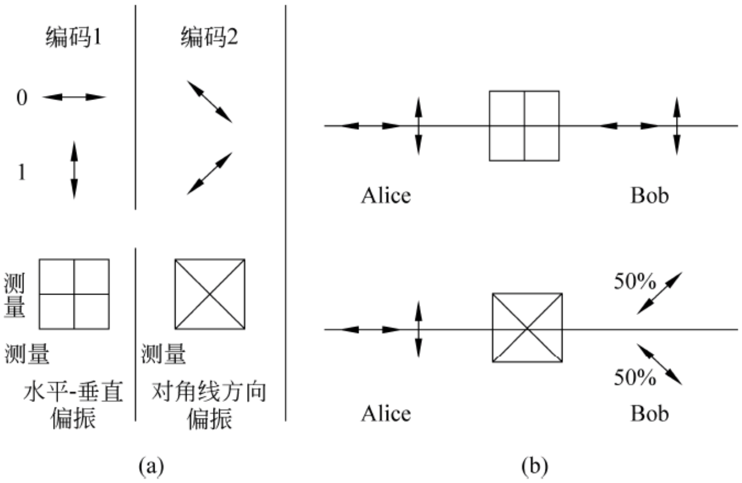

编码1
编码2
0
1
测量
测量
水平-垂直偏振
测量
对角线方向偏振
Alice
Bob
50%
50%
Alice
Bob
(a)
(b)

图7-13　单光子偏振态编码方式、测量基以及选用不同测量基的结果

1. BB84协议流程

具体的BB84协议流程如下(见图7-14)。

（1）单光子源产生一个一个的单光子。

（2）发送方Alice使用偏振片随机生成垂直、水平、＋45°或－45°的偏振态，将选定偏振方向的光子通过量子通道传送给接收方Bob。

（3）Bob随机选用两种测量基测量光子的偏振方向。

（4）Bob将测量结果保密，但将所用的测量基通过经典通道告知Alice。

（5）Alice 对比 Bob 选用的测量基与自己的编码方式，然后通过经典通道告诉 Bob 哪些基和她用的不同。

（6）Bob 扔掉错误基的测量结果（统计上会扔掉一半的数据）。

（7）Alice 和 Bob 选取一部分保留的密码来检测错误率，如果双方的 0、1 序列一致，则判定没有窃听者 Eve 窃听，剩下未公开的比特序列就留作量子密钥本。

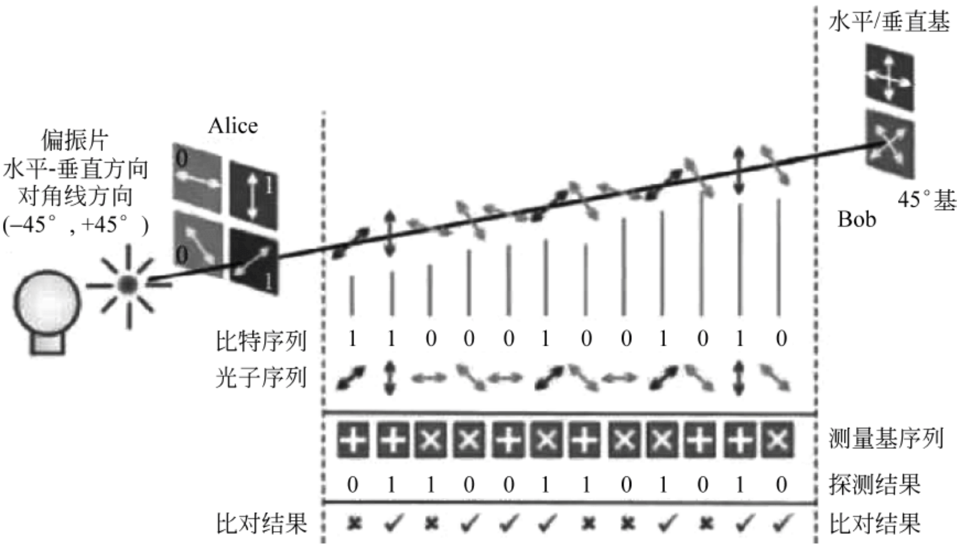

偏振片
水平-垂直方向
对角线方向
(–45°，+45°)
Alice
0
1
0
1
水平/垂直基
45°基
Bob
比特序列
1 1 0 0 0 1 0 0 1 0 1 0
光子序列
测量基序列
探测结果
0 1 1 0 0 1 1 0 1 0 1 0
比对结果
✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓
比对结果

图 7-14　BB84 协议流程

使用 BB84 协议进行 QKD，如果 Eve 想窃听，不仅需要窃听公开信道上的全部信息，还需窃听量子信道才能还原出最终的密钥。根据量子力学基本原理，当测量的量子态不是测量算符的本征态，会导致波包坍缩，从而破坏初始的量子态。

所以，Eve 如果冒充 Bob 劫持量子信道，由于她也不知道测量基，必然有 50％ 的测量结果也不准，而她还得冒充 Alice 把所测偏振态发送给 Bob，所以，Alice 和 Bob 在抽检比特串时会发现至少 25％ 的误码率。同时，由于量子不可克隆原理（处于未知的量子态的单量子态不可 100％ 精确复制），Eve 无法克隆 Alice 发送的单光子。Bob 和 Alice 通过检测误码率来判断是否存在窃听者 Eve；若发现被窃听，就停止通信。因此，BB84 协议从原理上是绝对安全的 QKD 协议。

2. BB84 协议现状

在实验上，BB84 协议依赖于多项技术条件，如高效产出的单光子源、无噪声干扰量子信道以及能高效读出单光子态的探测器；同时还要求通信双方选择发送、测量基的随机性品质好，最好采用真随机数调制。然而现实中有很多不理想情况，攻击者可利用这些漏洞进行攻击。情况如下。

（1）实际中的单光子源效率低，品质差，会有一定几率的多光子，这个现象可被利用进行光子数分离攻击，例如，单光子源同时出现两个光子，一个被窃听者拿去，另一个传送到接收方，会造成接收方对泄密无感知。

（2）现实中单光子探测器效率低，“量子黑客”可以以此作为攻击点，在 BB84 态测量中对应某一个基的探测器，使它致盲，让它不能接收信号，使光子探测器只剩一个基。

（3）窃听者可针对伪随机数，实施木马病毒等经典攻击方法。

例如，一种基于原理上的攻击方式，将 BB84 单光子态近似量子克隆为两个态，一个保留，一个发送，引起的误差是 14% 左右，小于直接窃听的误差 25%，误差上的减少也可能导致攻击。

针对实验器件和方案中的漏洞，世界范围内各个实验组展开了很多新工作，使 BB84 协议从原理上安全走向可实用的技术。

3. 与 BB84 协议等价的 E91 协议

在 BB84 协议中，巧妙的是密钥比特是在异地同时产生的，Alice 起先并不知道会产生什么样的比特序列。密钥的来源也可以视为 Alice 和 Bob 提前共享一组最大纠缠态，如处于 n 个状态为$(|00\rangle + |11\rangle)/\sqrt{2}$ 的量子比特纠缠对。

基于纠缠光子对的 E91 协议由 Ekert 于 1991 年提出。量子纠缠态保证 Alice 和 Bob 在测量基相同的情况下，测量结果完全一致（对应），结果与直接发送 BB84 单光子态一样，所以两个协议可视为等价的。

7.4.3　量子保密通信进展以及墨子星

从 1991 年开始，世界各国就开始了 QKD 实验。各国 QKD 早期实验情况如表 7-1 所示。

表 7-1　世界各国早期 QKD 实验

实验媒介	单位名称	年份	协议	量子态	波长/μm	距离	比特率/Hz	误码率/%
自由空间中	IBM Bennett	1991	BB84	偏振	0.55	32cm	1.2k	4
	中国科学院物理研究所	1995	BB84	偏振	0.56	30cm	4k	6
	Franson	1996	B92	偏振	0.633	150m	1k	2
	华东师范大学物理系	1997	B92	偏振	0.63;0.67	30cm	10k	6;2.1
	美国 Los Alamos	1999	B92	偏振	0.77	500m	5k	1.6
光纤中	英国 DRA	1992	E91	相位	0.883			
	英国 BT Labs	1993	BB84	相位	1.3	10km	20k	
	美国 Johns Hopkins	1995	BB84	偏振	0.633	1km	5k	0.4
	瑞士 Geneva Univ	1995	BB84	偏振	1.3	23km		0.54
	英国 BT Labs	1995	BB84	相位	1.3	30km	30k	4
	美国 Los Alamos	1999	BB84 B92	相位	1.3	48km	10	9.3

目前,QKD 技术已经进入实用阶段,世界上各个国家有很多应用实例,特别是在安全网络领域。2005 年,美国军方 DARPA 项目最早实现光开关技术和可信中继技术的组网结合,并建成包括 10 个节点的量子保密通信网络。2008 年,维也纳建成跨越 12 个国家,41 个小组的全可信任中继网络——欧洲 SECOQC 网络。日本也于 2010 年建成东京量子保密通信网。美国 Los Alamos 实验室自 2011 年以来一直使用内部的 QKD 网络。

要使用 QKD 技术实现广域量子保密通信,需要三级量子网络。首先通过光纤实现量子城域网络;然后通过可信中继器实现城际量子通信网络;最后通过卫星中转实现远距离的量子通信网络。

从历史上看,密码技术的每次进步都已经被破解技术的进步所打败。量子密钥分发终结了这场战斗。就像现代计算机中用以打开加密文件的密码一样,量子密钥也是一些长字符串,但它们被编码在量子粒子的物理状态中。这意味着它们不仅受计算机极限的保护,同时还受物理学定律的保护。

未来全球量子通信网络构想图如图 7-15 所示。

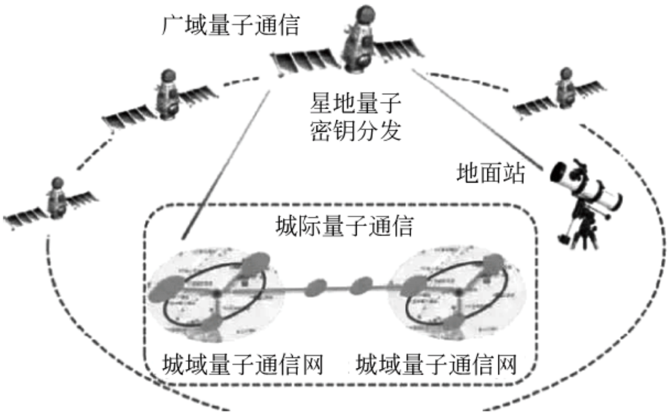


图 7-15　未来全球量子通信网络构想图

中国在量子保密通信领域走在了世界的前沿，先后在合肥、北京、济南实现了城市内QKD 网络；贯穿多个城市的城际通信网络“量子京沪干线”已于 2016 年年底开通。同时，世界首颗量子卫星“墨子号”于 2016 年 8 月 16 日在我国酒泉卫星发射中心成功升空。量子通信网络已经从城域、城际开始迈向星地一体的进程。

“墨子号”升空的第一要务是借助科学卫星，进行星地 QKD。除此之外，“墨子号”还进行多个量子力学实验，包括进行广域的量子纠缠分发、量子远程传态，以及量子力学完备性检验等实验研究。墨子星升天是向建设广域量子保密通信网络迈出的重要一步。未来，将有更多量子通信卫星与之携手作战，从而实现全球化的广域量子保密通信网络，我们期待着这一天的到来。“墨子号”量子通信卫星模型如图 7-16 所示。

现在，量子密钥可以通过卫星传输，对相隔万里的城市间发送的信息进行加密。研究人员对照片进行量子加密后，将它们成功地在北京和维也纳之间进行了传输，传输距离达到约 7600km，远超之前在中国创造的 404km 的纪录。接下来，两座城市的研究人员又举行了历时 75 分钟的视频会议，也是通过量子密钥进行加密。

报道称，这种远距离量子密钥分发是中国的“墨子号”卫星的一个成就，该卫星在2017 年打破了多项纪录。不过，“墨子号”卫星同地球之间的联系仍非绝对安全。该网络设计的缺陷在于卫星本身。只要通信方相信没有怀有恶意的宇航员秘密闯入“墨子号”卫星本身，从源头读取量子密钥的话，这个系统就没有问题。

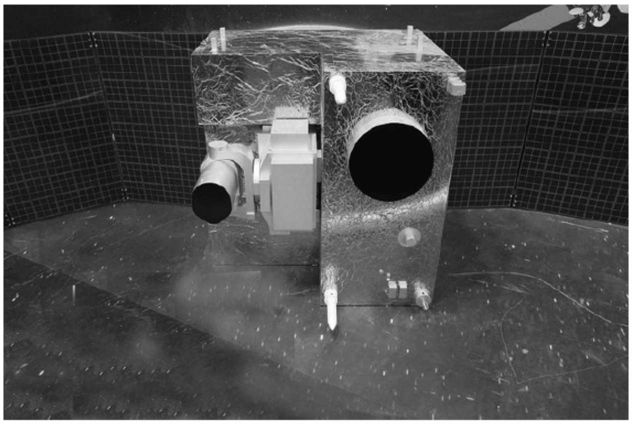


图 7-16 “墨子号”量子通信卫星模型

研究人员表示，他们计划发射更多量子卫星到更高的轨道上，这些卫星将可以彼此通信，并与地球上的研究人员在日益复杂的网络中通信。这一逐渐扩展、日益实用的量子网络首先将为中国和欧洲制造，然后再扩展到全球范围。

7.4.4 我怎么知道有人在偷听：光子的偏振态

1. 量子通信为啥就能发现窃听者

现代量子信息理论与实验的快速发展，使得量子通信保密性很好，一旦有人试图打开信件，量子密钥会让信件自毁，解释如下。

量子理论认为，微观领域里，某些物质可以同时处于多个可能状态的叠加态，只有在被观测或测量时，才会随机地呈现出某种确定的状态。因此，对物质的测量意味着干涉，改变被测量物质的状态。

基于这一原理，科学家们提出量子密码的概念，也就是用具有量子态的物质作为密码。这样一来，任何截获或测试量子密码的操作，都会改变量子状态。换言之，截获量子密码的人得到的只是无意义的信息，而信息的合法接收者也可以从量子态的改变中知道量子密码曾被截取过。量子密码被应用于量子通信系统中，便是“量子保密通信”。

与经典保密通信不同，量子密钥分发的安全性是由量子力学的基本原理所保证的，它利用海森伯测不准原理和量子态不可克隆定理，将量子态作为信息的载体，利用一系列的

密钥协商过程，对量子信息进行运算处理，从而获得只有收发两端可知的密钥，在此之后，再对要传送的信息进行加密与解密，并将其在经典信道上进行传输。量子密钥分发协议模型如图7-17所示。

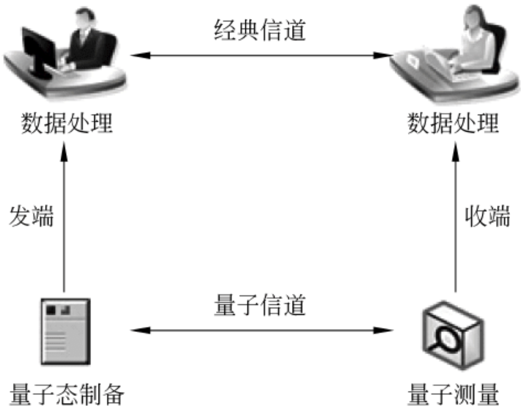


图 7-17　量子密钥分发协议模型

在此过程中，海森伯测不准原理使窃听方只能以一定概率获取所截获的信息，而根据量子特性，这种截获将会导致量子态的改变，从而使误码率大大提高，而这一变化将被密钥协商的收发双方所发现，保证了密钥协商过程的安全性。

量子态不可克隆定理，使窃听方不能通过将信息先复制先来的手段进行窃听，从而保证了在量子信道上传输信息的唯一性。

所以，量子密钥分发与经典保密通信最大的不同就在于，它并非单纯地利用计算复杂性使窃听者无法在有限的时间内对密码进行破译，而是运用量子力学的基本原理以及量子特性去寻找窃听者是否存在，从而使通信双方较窃听者有更高的信息优势，最终确保了通信的安全。

总之，通过近20年的研究，量子通信保密技术有了突飞猛进的发展，其理论框架已基本形成，理论体系也日趋完善，不但在理论技术上有了很大的进步，而且在产品研制方面也取得了丰硕的成果。在未来，量子通信安全性必将会朝着网络化与实用化继续发展，为人们的生活带来更大的便利。

2 量子密码的主要方法就是量子密钥分配

量子密码的一个主要方法就是利用量子态产生密钥,这就是量子密钥分配。注意,最后得到的密钥本身仍然是经典的。

量子密钥分配的一个主要方案是1984年提出的BB84方案。下面用光子的偏振态解释。

假设两个人A和B要确定一组共享的密钥。A先随机地用$|\leftrightarrow\rangle|\leftrightarrow\rangle$或者$|\nearrow\rangle|\nearrow\rangle$代表0,并随机地用$|\updownarrow\rangle|\updownarrow\rangle$或者$|\searrow\rangle|\searrow\rangle$代表1。A以此方法产生一批光子,发送给B。B对于每个光子测量其偏振态,每次测量又都是随机选择$|\leftrightarrow\rangle|\leftrightarrow\rangle$和$|\updownarrow\rangle|\updownarrow\rangle$这组基或者$|\nearrow\rangle|\nearrow\rangle$和$|\searrow\rangle|\searrow\rangle$这组基。

然后A和B交流,对于每个光子的产生和测量,分别是用了哪组基,但不说明具体的态。他们的这个交流不需要保密,可以是公开的。然后将产生和测量用的基不一样的情况剔除,剩下的光子的偏振态在A发出和B测量后应该是一样的,而且别人不知道。

理想情况下,这些光子既然产生与测量的基一致,那么它们在B测量后的偏振态也就应该与在A处产生时一样,除非被“窃听”过。假设某个光子曾在传输途中被E截留,E测量其偏振态,然后再发给B,这就是“窃听”。

E当时不知道该光子是通过哪组基产生的。假设他随机地选择这两组基之一来测量。如果E测量所用的基碰巧与光子在A处产生时的基一致(有1/2概率是这样),那么E就会正确地测量得到光子的偏振态,而且未作改变,又发给了B。

这样,光子的偏振态就与没有被窃听的情况一样。B收到该光子后,如果用与A一样的基测量,得到的结果就与光子产生发出时的偏振态一样。E的窃听就不能被发现。但是如果E窃听时用的基与原来的不一样(有1/2概率是这样),那么测量之后,光子偏振态就改变了,变成E测量所用的基上的两个基矢态之一。

B收到该光子后,如果用与A一样的基测量,那么其中只有1/2概率得到的结果与产生时一样。另有1/2概率得到的结果与产生时的偏振态相正交,这就出错了。这些概率是计算出来的。因此总的来说,如果存在窃听,就会引起可观的错误率,在上述窃听方案下,引起的错误率是1/4。

因此，A 和 B 可以从产生与测量所用的基相同的光子中选择一部分来做抽查。将它们产生与测量的偏振态做比较。如果没有被窃听过，这些光子被 B 测量得到的结果应该与在 A 出产生时一样。而如果被窃听过，其中有一些光子的偏振态就有变化。如果 E 每次窃听是完全随机选择这两套基中的一个，那么偏振态发生变化的光子占 1/4。由此 A 和 B 可以判断出是不是存在窃听。

这个方案的保密性基于不同的基之间的不相容，即互为叠加态。

7.5　量子密码的宝典——工作原理

量子密码术用我们当前的物理学知识来开发不能被破获的密码系统，即如果不了解发送者所使用的密钥，接收者几乎无法破解并得到内容。

7.5.1　宝典一：量子密码理论模式

理论上，量子密码术工作在以下模式：假设两个人想安全地交换信息，命名为 Alice 和 Bob。Alice 通过发送给 Bob 一个键来初始化信息，这个键可能就是加密数据信息的模式，是一个随意的位序列，用某种类型模式发送，可以认为两个不同的初始值表示一个特定的二进制比特(0 或 1)。

我们暂且认为这个键值是在一个方向上传输的光子流，每一个光子微粒表示一个单个的数据位(0 或 1)。除了直线运行外，所有光子也以某种方式进行振动。这些振动沿任意轴在 360°的空间进行着，为简单起见(至少在量子密码术中可简化问题)，我们把这些振动分为 4 组特定的状态，即上、下，左、右，左上、右下和右上、左下，振动角度就沿光子的两极。过滤器允许处于某种振动状态的原子毫无改变地通过，令其他的原子改变振动状态后通过(它也能彻底阻塞光子通过，但在这里将忽略这一属性)。Alice 有一个偏光器允许处于这四种状态的光子通过，实际上，她可以选择沿直线(上、下，左、右)或对角线(左上、右下，右上、左下)进行过滤。

Alice 在直线和对角线之间转换她的振动模式来过滤随意传输的单个光子。这样时，

就用两种振动模式中的一种表示一个单独的比特，1 或 0。

当接收到光子时，Bob 必须用直线或对角线的偏光镜来测量每一个光子位。他可能选择正确的偏光角度，也可能出错。由于 Alice 选择偏光器时非常随意，那么当选择错误的偏光器后光子会如何反应呢？

我国实际建成的第一个量子密码网络系统（北京）如图 7-18 所示。

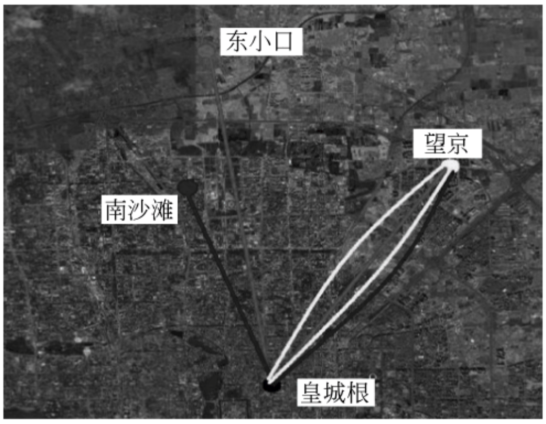


图 7-18　我国第一个量子密码网络系统（北京）

量子密码体系采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。量子密码的安全性由量子力学原理保证。

绝对安全性是指，即使窃听者可能拥有极高的智商、可能采用最高明的窃听措施、可能使用最先进的测量手段，密钥的传送仍然是安全的。

通常，窃听者采用截获密钥的方法有两类。

一种方法是通过对携带信息的量子态进行测量，从其测量的结果来提取密钥的信息。但是，量子力学的基本原理告诉我们，对量子态的测量会引起波函数坍缩，本质上改变量子态的性质，发送者和接收者通过信息校验就会发现他们的通信被窃听，因为这种窃听方式必然会留下具有明显量子测量特征的痕迹，合法用户之间便因此终止正在进行的通信。

另一种方法则是避开直接的量子测量，采用具有复制功能的装置，先截获和复制传送信息的量子态。然后，窃听者再将原来的量子态传送给要接收密钥的合法用户，留下复制

的量子态可供窃听者测量分析,以窃取信息。这样,窃听原则上不会留下任何痕迹。

但是,由量子相干性决定的量子不可克隆定理告诉人们,任何物理上允许的量子复制装置都不可能克隆出与输入态完全一样的量子态来。这一重要的量子物理效应,确保了窃听者不会完整地复制出传送信息的量子态。因而,第二种窃听方法无法成功。量子密码术原则上提供了不可破译、不可窃听和大容量的保密通信体系。

7.5.2　宝典二:量子密码理论分析

海森伯不确定原理指出,人们不能确定每一个单独的光子会怎样,因为测量它的行为时改变了它的属性(如果我们想测量一个系统的两个属性,测量一个的同时排除了对另外一个量化的权利)。然而,我们可以估计这一组发生了什么。

当Bob用直线测光器测量左上/右下和右上/左下(对角)光子时,这些光子在通过偏光器时状态就会改变,一半转变为上下振动方式,另一半转变为左右方式。但我们不能确定一个单独的光子会转变为哪种状态(当然,在真正应用中,一些光子会被阻塞掉,但这与这一理论关系不大)。

Bob测量光子时可能正确也可能错误,可见,Alice和Bob创建了不安全的通信信道,其他人员也可能监听。接下来Alice告诉Bob她用哪个偏光器发送的光子位,而不是她如何两极化的光子。她可能说8597号光子(理论上)发送时采用直线模式,但她不会说发送时是否用上、下或左、右。Bob这时确定了他是否用正确的偏光器接收了每一个光子。

然后Alice和Bob就抛弃他利用错误的偏光器测量的所有的光子。他们所拥有的,是原来传输长度一半的0和1的序列。但这就形成了One-Time Pad(OTP)理论的基础,即一旦被正确实施,就被认为是完全随意和安全的密码系统。

7.5.3　宝典三:量子密码假设

我们假设有一个监听者Eve,尝试着窃听信息,Eve有一个与Bob相同的偏光器,需要选择对光子进行直线或对角线的过滤。然而,他面临着与Bob同样的问题,有一半的可

能性他会选择错误的偏光器。Bob 的优势在于他可以向 Alice 确认所用偏光器的类型。而 Eve 没有办法，有一半的可能性她选择了错误的检测器，错误地解释了光子信息来形成最后的键，致使其无用。

而且，在量子密码术中还有另一个固有的安全级别，就是入侵检测。Alice 和 Bob 将知道 Eve 是否在监听他们。Eve 在光子线路上的事实将非常容易被发现，原因如下。

假设 Alice 采用右上/左下的方式传输编号为 349 的光子给 Bob，但这时，Eve 用了直线偏光器，仅能准确测定上下或左右型的光子。

如果 Bob 用了线型偏光器，那么无所谓，因为他会从最后的键值中抛弃这个光子。但如果 Bob 用了对角型偏光器，问题就产生了，他可能进行正确的测量，根据海森伯不确定性理论，也可能错误的测量。Eve 用错误的偏光器改变了光子的状态，即使 Bob 用正确的偏光器也可能出错。

一旦发现了 Eve 的恶劣行为，他们一定采取上面的措施，获得一个由 0 和 1 组成的唯一的键序列，除非已经被窃取了，才会产生矛盾。这时他们会进一步采取行动来检查键值的有效性。如果在不安全的信道上比较二进制数字的最后键值是很愚蠢的做法，也是没必要的。

假设最后的键值包含 4000 位二进制数字，Alice 和 Bob 需要做的就是从这些数字当中随机地选出一个子集（200 位吧），根据两种状态（数字序列号 2、34、65、911 等）和数字状态（0 或 1），进行比较，如果全部匹配，就可以认为 Eve 没有监听。

如果她在监听，那么不被发现的概率是万亿分之一，也就是不可能不被发现。Alice 和 Bob 发现有人监听后将不再用这个键值，他们将在 Eve 不可到达的安全信道上重新开始键值交换，当然，上述的比较活动可以在不安全的信道上进行。如果 Alice 和 Bob 推断出他们的键值是安全的，因为他们用 200 位进行了测试，这 200 位将被从最后的键值中抛弃，4000 位变为了 3800 位。

因此，量子加密术在公共的键值密码术中是连接键值交换的一种相对较容易、方便的方式。

7.6　人人都有的秘密——量子密钥分发

7.6.1　量子密钥分配的远程通信

目前，采用诱骗态方法的量子密钥分配最远实验距离是260～300km。

尽管随着检测技术的提高，该距离还会进一步提高，但由于成码率随着距离呈指数衰减，而单量子态信号又不能在中途放大，因而基于经典相干态光源的诱骗态方法很难直接完成远程量子通信任务。

远程量子通信的实现将依赖于中继站。目前，中继分为量子中继和可信中继两种。

量子中继以量子纠缠分发技术先在各相邻站点间建立共享纠缠对，以量子存储技术将纠缠对存储，采用远距离自由空间传输技术实现量子纠缠转换。

中国研究人员已在固态系统中首次实现对三维量子纠缠态的量子存储，保真度高达99.1%。

例如，将量子纠缠对布置在各相邻站点，纠缠转换操作后便可实现次近邻站点间的共享纠缠，理论上可以实现远程量子通信，但量子中继技术难度非常大，目前还做不到。

可信中继类似于量子密钥接力赛，是A把密钥传输给B，B再把密钥传输给C，中途密钥要落地，B是知道密钥的所有信息的，因此要求中继必须可信，如果一个中继站被窃听者控制，那么就无法保障量子通信的安全性。

相比较而言，量子中继在中途密钥是不落地的，拥有更好的安全性，但目前的技术达不到这方面的技术要求，已经产业化的是可信中继。

虽然量子密钥分配相对于量子隐形传态的科幻程度和技术难度都要低不少，但其更具产业化前景，技术更成熟的优势也是显而易见的。

7.6.2　云中漫步安全保障：量子保密通信系统

量子通信指利用量子效应加密并进行信息传输的一种通信方式。

量子通信主要涉及量子密码通信、量子远程传态和量子密集编码等，这门学科已逐步

从理论走向实验，并向实用化发展。高效安全的信息传输日益受到人们的关注。基于量子力学的基本原理，量子通信具有高效率和绝对安全等特点，并因此成为国际上量子物理和信息科学的研究热点。

1. 量子通信系统的基本部件

量子通信系统的基本部件包括量子态发生器、量子通道和量子测量装置。按其所传输的信息是经典还是量子而分为两类。前者主要用于量子密钥的传输，后者则可用于量子隐形传态和量子纠缠的分发。隐形传送指的是脱离实物的一种“完全”的信息传送。

从物理学角度，可以这样来想象隐形传送的过程：先提取原物的所有信息，然后将这些信息传送到接收地点，接收者依据这些信息，选取与构成原物完全相同的基本单元，制造出原物完美的复制品。但是，量子力学的不确定性原理不允许精确地提取原物的全部信息，这个复制品不可能是完美的。因此，隐形传送不过是一种幻想而已。

2. 利用经典与量子相结合的方法实现量子隐形传态的方案

1993 年，6 位来自不同国家的科学家，提出了利用经典与量子相结合的方法实现量子隐形传态的方案：将某个粒子的未知量子态传送到另一个地方，把另一个粒子制备到该量子态上，而原来的粒子仍留在原处。其基本思想：将原物的信息分成经典信息和量子信息两部分，它们分别经由经典通道和量子通道传送给接收者。

经典信息是发送者对原物进行某种测量而获得的，量子信息是发送者在测量中未提取的其余信息；接收者在获得这两种信息后，就可以制备出原物量子态的完全复制品。该过程中传送的仅仅是原物的量子态，而不是原物本身。发送者甚至可以对这个量子态一无所知，而接收者是将别的粒子处于原物的量子态上。

在这个方案中，纠缠态的非定域性起着至关重要的作用。量子力学是非定域的理论，这一点已被违背贝尔不等式的实验结果所证实，因此，量子力学展现出许多反直观的效应。在量子力学中能够以这样的方式制备两个粒子态，在它们之间的关联不能被经典地解释，这样的态称为纠缠态，量子纠缠指的是两个或多个量子系统之间的非定域、非经典的关联。量子隐形传态不仅在物理学领域对人们认识与揭示自然界的神秘规律具有重要

意义，而且可以用量子态作为信息载体，通过量子态的传送完成大容量信息的传输，实现原则上不可破译的量子保密通信。

为了进行远距离的量子态隐形传输，往往需要事先让相距遥远的两地共同拥有最大量子纠缠态。但是，由于存在各种不可避免的环境噪声，量子纠缠态的品质会随着传送距离的增加而变得越来越差。因此，如何提纯高品质的量子纠缠态是量子通信研究中的重要课题。

7.7　量子安全直接通信

已完成的“多自由度量子隐形传态”和北京到上海的2000km量子通信干线，虽然都被归入量子通信范畴，但其实是两种不同的技术。

量子通信在定义上存在争议。目前，量子密钥分配和量子隐形传态都被称为量子通信。

量子密钥分配可以建立安全的通信密码，通过一次一密的加密方式可以实现点对点方式的安全经典通信。

具体做法是用弱相干光源发射光子，因为弱相干光源弱到一定程度，光子是一个一个往外蹦的，以此代替单光子源。把一个信息编码在一个光子上，一个光子有着不同的量子态，代表着0和1，把光子通过光纤发射过去，接收方接到密钥后进行解码。

本质上说，量子密钥分配其实依旧依托于光纤通信，而单光子具有不可分割性是量子密码安全性的物理基础，因而量子密钥分配并非颠覆经典通信，更像是给经典通信增加了一把量子密码锁。

现有的量子密钥分发技术可以实现实验室状态下200km以上的量子通信，再辅以光开关等技术，还可以实现量子密钥分发网络。目前，开始产业化的就是量子密钥分配，而不是量子隐形传态，比如之前提到的北京到上海的2000km量子通信干线，以及沪杭量子通信干线、陆家嘴量子通信金融网等。

量子态隐形传输是基于量子纠缠态的分发与量子联合测量（量子纠缠是指两个量子

态具有相干性或处于关联状态，量子纠缠态分发是指制备纠缠粒子对，将不同的粒子对发往不同的地方)，在经典通信的辅助下实现量子态的空间转移而又不移动量子态的物理载体。

虽然在量子隐形传态技术上中国走在美国的前列，但现在仅仅是技术突破，离产业化还非常遥远。

第8章

量子计算机的“社会分工”

8.1 世界是我们的也是你们的：传统计算机渐渐接近它们的极限

在这一节里希望和大家共同探讨传统计算机的极限这个话题。

接下来在工程、功耗、时空概念、复杂理论及新兴技术等方面探讨计算机的极限，以及面对这些极限，计算机科学家们所采取的措施。下面，先从工程方面讨论。

8.1.1 近20年芯片的发展速度几乎没有提升

从1958年第一个仅包含一个双极性晶体管的集成电路问世，到如今集成十几亿晶体管的处理器芯片，集成电路在近60年的时间里发展迅速。我们现在用的手机的性能也已经相当于30年前的Cray-2超计算机了，然而手机的功耗却只有Cray-2的十万分之一，价格更是被降到大多数普通人能接受的程度。如此巨大的发展速度的背后是怎样的规律呢？30年后我们也能每人手里拿个“天河2号”吗？要说清楚这个问题就不得不提到芯片产业最著名的摩尔定律。

摩尔定律由摩尔于1965年在《电子学》杂志中提出，之后摩尔于1968年和罗伯特·诺伊斯共同创办Intel公司，时任副总裁。在公司创办之前，摩尔发现半导体晶体管制程的发展速度对于芯片制造业非常重要。如果发展过慢，不但芯片的制作成本不会得到有效的分散，公司还会面临被竞争对手淘汰的风险。如果倾其所有研究晶体管的制程，一旦研究失败对公司的打击也是毁灭性的。

于是当时的芯片生产行业都在试图寻找一个合适的发展速度，使得在公司利润最大化的同时能够继续分配一部分利润出来维持这个发展速度。在研究了当时晶体管制程的发展之后，摩尔在1965年提出了摩尔定律：同面积的集成电路上可容纳的晶体管数量会以每年增加一倍的速度发展。

在10年之后的1975年，摩尔在“IEEE国际电子元件大会”上发表论文*Progress in Digital Integrated Electronics*，根据当时的实际情况对摩尔定律做出第一次修正，将每年增加一倍改为每两年增加一倍。摩尔定律作为一个经验法则为芯片生产商提供了一个利润和风险的折中，而半导体行业也遵循这个法则进入一个良性的发展。

Intel公司的执行副总裁William M. Holt在2016年的ISSCC会议上比较了十年内按照摩尔定律发展新制造过程和一直使用旧的制造过程生产芯片这两种生产方式，发现前者的芯片生产成本仅是后者的40%，而摩尔定律毕竟是一个经验法则，在1975年第一次修正之后，半导体行业在摩尔定律的指导下一直发展到2013年。ITRS(International Templar Research Society)在2013年将摩尔定律进行了第二次修正，将之前每两年翻倍的发展速度改成了每三年翻倍。

这次修正从工程的角度来看至少有四个原因。

1. 工艺的极限

现在的半导体制造工艺中很重要的一个部分是光刻。光刻利用曝光和显影在光刻胶层上画几何图形，然后通过刻蚀工艺将光掩膜上的图形转移到其所在的衬底上。这种工艺在理论上受阿贝分辨率的限制。简单地说，由于可见光的波动性使其可以发生衍射，光束不能无限聚焦。而分辨率的极限值大约在$2\lambda n$，其中λ是光刻所用的激光波长，n是介质的数值孔径。数值孔径目前在光学中能达到的极限是1.4，那么光刻精度的极限就是2.8λ。

如此看来，要实现更小的工艺制作，就要用到波长更短的激光，而短波长的激光利用起来本就非常复杂。虽然科学家提出了新的工艺技术，使得现在的光刻工艺突破了阿贝分辨率的限制，能够使用波长是193nm的激光做出14nm的工艺，这种工艺技术也大大提高了制作成本。无论是在阿贝分辨率的限制下利用更短波长的激光；还是开发出新技术

来突破阿贝分辨率的限制，把单个晶体管做到更小（即在同面积的集成电路上容纳更多的晶体管）变得异常困难。

2. 内部连接的极限

随着单位面积集成电路中的晶体管越来越多，内部连接成了集成电路中越来越重要的部分。内部连接要么做到快速的信号传输；要么做到用尽量细的铜线和密集的排布（从而做到更小的集成电路设计），但鱼和熊掌不能兼得。

因为更细的铜线会增加铜线的电阻，而更密集的排线也会使铜线间电流的相互影响。早在1995年Intel的研究员们就指出了真正限制集成电路发展的是其内部的连接技术。为了解决这个问题，科学家们提出了光波导管的概念来替换传统的铜线连接方式。这种内部连接的方式也受麦克斯维尔方程的理论限制，例如电磁波传输的速度上限。所以，即便是晶体管能够越做越小，如何在保证快速信号传输的同时加入更多的内部连接也成为了一个非常棘手的问题。

3. 传统晶体管的设计极限

当晶体管尺寸做到10nm时，晶体管的栅氧化层仅仅只有几个原子的厚度。在这个尺度下至少会有三个问题：

(1) 在量子隧穿效应的影响下，晶体管的性质将变得很不稳定。

(2) 因为每个晶体管的制造过程不可能完全一样，每个晶体管会有不同的特性，而产生的不同特性在纳米级的尺度下会更加明显。

(3) 晶体管将会发生严重漏电。这对移动设备兴起的今天来说是一个相当大的问题。毕竟谁也不希望自己的手机充电两小时，通话五分钟。

因为量子效应在10nm左右的尺寸下介入，将传统晶体管做到这个尺度以下将会变得难上加难。当然，科学家为了突破这个极限也提出很多新的晶体管设计，其中比较成熟的有鳍式场效应晶体管（Fin-Effect Transistor，FinFET）和隧道晶体管（Tunneling Transistor）。

FinFET在传统晶体管的基础上通过三维设计增加栅氧化层的宽度；Tuneling Transistor更是提出了控制量子隧穿的办法。但这些技术方面的改进也同样需要大量的

资本投入，因此，放缓了之前摩尔定律设定下的发展速度。

4. 技术投入的极限

之前提到科学家们面临各种物理极限时在晶体管制作工程方面提出的改变，正是这些改变的措施造成了这第四项极限。新科技的研发需要大量的资金以及时间，即便是研发成功，公司的技术人员也需要投入大量的精力去学习并使用这些新的技术。这就导致了很多中小芯片制造商无力承担新技术的投入，而转向继续使用旧技术进行生产加工。

正是因为这些中小芯片厂商大量退出新技术的研发，芯片产业的发展在到达原有技术的理论极限之后又遇到了发展的瓶颈，发展速度也因此明显放缓。这也是导致2013年国际半导体技术蓝图组织（International Technology Roodmap for Semiconductors，ITRS）对摩尔定律进行了第二次修正的原因之一。

所以，单纯将晶体管做小这条路不会一直走下去，而摩尔定律在今后的某个时间段可能会再一次遇到瓶颈。所以，我们在30年后拥有“天河2号”计算能力的手机的理想也不太可能实现。然而这一切似乎并不代表着结束，面对这一工程上面的限制，业界提出了一种新的发展方向——超越摩尔定律。持有这个观念的计算机科学家们逐渐转向了对计算机体系结构的研究，更加侧重于功能的多样化，更多地靠电路设计及系统算法进行优化。

于是，研究者们开始通过更高维度来寻找可能性。就像当一个城市的道路无法满足人们的需求时就会出现地铁和高架桥。在二维工艺受限时，人们便开始探索三维集成电路。例如，把处理器和内存上下堆叠，使用封装内走线来代替传统的二维平面走线作为连接。这种三维结构不仅通过封装内走线的高密度性增加了内存访问带宽，同时也因为减少了连接长度而减少了数据访问的延迟。

所以，正如FinFET之父胡志明所说：“即便是面对如此之多的理论限制，半导体的发展并没有进入尾声，产业的进步需要我们通过不断地改进，过去五十年是这样走过来的，相信未来五十年也会这样走下去。”

8.1.2 登纳德定律中一直在“偷懒”的芯片

什么是登纳德缩放比例定律？为什么芯片里总有那么一部分甚至一大部分是不能同

时工作的？为什么我们还要费尽心思往集成电路里加更多的晶体管呢？暗硅又是一种什么概念？

早在1971年，Intel公司推出了首个商用但速度仅有740kHz的计算机芯片Intel C4004。Intel C4004微处理器如图8-1所示。在此之后，芯片速度得到了迅速发展，在不到30年后的2000年就已经突破了2GHz，达到了近3000倍的增长。然而从2000年开始，芯片发展速度开始放缓，直到如今市场上多数处理器也在3GHz左右徘徊。

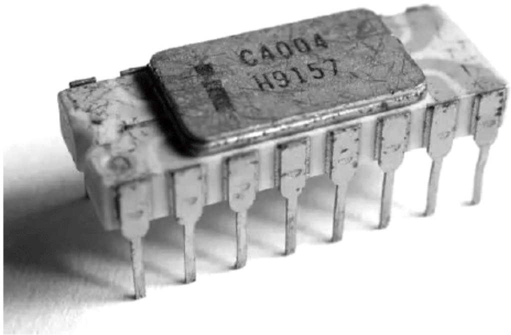


图8-1　Intel C4004微处理器

2001年，IBM公司首先制造出了世界上第一个双核处理器，使得两个低速度、低功耗的处理器能在性能方面与当下的单个高速度的处理器相匹敌，并由此开辟了并行化体系结构的市场。

2004年，在AMD公司发布了其第一个双核处理器之后，Intel公司更是宣布取消其对4GHz处理器的研究，与当时一众同行一起投入到了多核处理器的研发当中。由此，计算机芯片的发展从之前的更高速的单核研究转变到了同等甚至更低速的多核研究。究其原因，主要来自于更高速的处理器的功耗和散热问题已经达到了必须解决的程度。

2013年，ITRS在第二次修正摩尔定律的同年发表评论，将功耗问题列为了计算机发展的主要挑战。那么这个挑战从何而来呢？为什么在如此迅速发展之后突然遇到门槛呢？这就不得不提到芯片行业发展的又一个定律——登纳德缩放比例。

在了解登纳德缩放比例定律之前，我们先来看看晶体管的功耗是如何计算的。晶体管的功耗大体分为两类：一类是静态功耗；另一类是动态功耗。静态功耗的计算比较好

理解，就是常规的电压乘以电流。晶体管在做 1 和 0 的相互转换时会根据转换频率的高低产生不同大小的功耗，人们把这个功耗称为动态功耗，动态功耗与电压的平方以及频率成正比。

1974 年，也就是摩尔第一次修正摩尔定律的前一年，登纳德在发表的论文 *Design of Ion-implanted MOSFETS with Very Small Physical Dimensions* 中表示，晶体管面积的缩小使得其所消耗的电压以及电流会以基本相同的比例缩小。也就是说，如果晶体管的大小减半，该晶体管的静态功耗将会降为之前的四分之一（电压电流同时减半）。

芯片业的发展目标基本上是在保证功耗不变的情况下尽可能提高性能。那么根据登纳德缩放比例，设计者可以大大地提高芯片的时钟频率，因为提高频率所带来的更多的动态功耗会和减小的静态功耗相抵消。于是，登纳德缩放比例定律同摩尔定律一起引领了芯片行业 30 多年的飞速发展。因为在往同面积电路中集成更多晶体管时，提高芯片时钟频率成为了一个“免费的午餐”。

事情发展到 2005 年前后。在摩尔定律的指导下，当晶体管越做越小时，量子隧穿效应（指像电子等微观粒子能够穿入或穿越位势垒的量子行为）开始慢慢介入，使得晶体管漏电现象开始出现。漏电现象的出现打破了原先登纳德所提出的定律，使得晶体管在往更小工艺制作时候的静态功耗不减反增，同时也带来了很大的热能转换，使得芯片的散热成为急需解决的问题。

如果散热做得不好，芯片的寿命将变得不稳定甚至大大减少。在这种情况下，提高芯片的时钟频率不再是“免费的午餐”。相反，在没有解决晶体管漏电的问题之前，单纯的增加芯片的时钟频率因散热问题无法解决而变得不可实现。

于是芯片研究商们开始纷纷停止高频芯片的研发，而转向低频多核架构的研究。这才有了从 2001 年开始的第一个双核芯片到现在个人计算机的 4 核芯片，再到如今 Intel 公司最新架构 KnightLanding 上的 64 核芯片的发展。

然而，单核向多核的发展并没有从根本上解决问题。因为芯片研发商仅仅是停止了高频单核的研发，但并未停止往同面积的集成电路内加入更多的晶体管。不然就不会有从双核到四核再到八核的发展了。正如之前所提到的，在登纳德缩放比例不再适用、晶体

管越做越小并因晶体管漏电而导致芯片发热越来越严重的今天，芯片制造商们又是如何解决功耗以及散热的问题呢？答案是没有解决！可能你引以为傲的八核处理器只不过是一个摆设。要解释这个问题，就需要了解“暗硅”这个概念。

“暗硅”这个概念是2011年在计算机体系结构会议ISCA中首次提出的。研究员发现在后登纳德时代，为了在现有的散热技术上保证芯片不至于过热、功耗不至于过大，如今多核芯片中已经有一部分不能和其余部分同时使用。举个简单的例子，对于一个65nm下的4核处理器，假如额定功耗允许其四个核能够同时全速工作。当工艺缩小到32nm时，等面积的处理器现在能容下16核，但是能够同时工作的还是只有四个核。这块不能和其他部分同时使用的12个核就称为暗硅。

按照如今的发展速度，现代处理器的暗硅部分很快就能达到99%。也就是说，不久之后的芯片，即便是再先进，在同一时间能够利用的也只是1%。加上越来越多核数的集成，内部连接所导致的功耗也正在逐渐超过核内运算所导致的功耗。基于这个结果，Microsoft和IBM公司共同预测了多核芯片研发在不久的将来即将终结。

那么问题来了，既然芯片大部分会成为暗硅，那么芯片商为什么还要不断地往同面积的芯片上加入更多的核呢？为什么不通过把芯片直接做小来减少成本呢？首先芯片面积的成本根本不重要。随着芯片越做越小，芯片的面积成本所占的比重越来越小，从而使得芯片成本不会因为芯片面积缩小而线性缩小。

芯片的引脚和封装开始占据设计成本中越来越重要的部分。其次就是商业原因。尽管多出来的核数大多数都是暗硅，但八核处理器听起来就是比双核先进，容易在消费者心里留下更深的印象。而且通过一些程序和编译器的优化设计也确实有可能让更多的核在更低频的工作，从而达到系统性能的提升。至少八核处理器的潜力大过双核，特别是对一些特殊任务的加速。虽然这些特殊的任务不常遇到。

面对这些问题，科学家们又是怎么应对的呢？在业界，ARM率先提出了异构系统架构，在芯片里同时放入大核（高频）与小核（低频）。核的利用根据所运行的程序由操作系统决定，从而达到尽量减小功耗的目的。

8.1.3 多核的陷阱：从程序的角度探讨计算机的极限

前面分别从工程和功耗两个方面讨论了计算机的极限问题，并由此分别引出了摩尔定律及登纳德缩放比例定律。下面我们暂时抛开硬件，从程序的角度解释系统并行化的极限。

上面讲到，在功耗非线性增长的压力下，芯片厂商开发出多核芯片，试图通过多核来解决之前单核的时钟频率增加所带来的功耗问题。然而这种决定忽略了另外一个很重要的问题。要讲清楚这个问题，我们先来讲个故事。

从前有一个不知足的地主，之前都是雇一个长工耕田。这个长工也很配合，随着时间的推移，技术越来越好，耕田也越来越快。但有一天这个长工达到了体能极限，于是地主就琢磨着他这块田怎么能再快点耕完。终于有一天地主下了血本从市场上又雇了另外三个技能相当的长工，并满心希望之前一天能耕完的地现在六个小时就可以耕完。于是地主六个小时之后去地里一看，瞬间后悔了。因为刚雇来的三个长工也不知道自己该做什么，就坐在边上看着原先的那位长工卖力地工作。

故事讲到这里，可能有心的读者就已经发现了多核处理的问题。就是在此之前的绝大多数程序都是按照串行算法开发的，而这些程序还不能很好地在多核芯片上并行执行。因为整个程序里并没有启用多余的核进行处理，而这些多余的核在大多数时间里也都是空闲的。当然需要说明的是，这种情况只在执行单个程序时发生，如果是执行多个不同的程序，那么多核还是会有效果的。就像如果这个地主有四块地分别分给雇来的四个长工，他们还是可以有效工作的。

于是学术界和产业界开始了又一波对并行化的研究。他们一部分人希望通过设计新的编程语言，让程序员人工提高程序的并行度。另一部分人则希望通过对编译器的优化，让编译器自动识别程序中可并行的部分并生成可并行的二进制码。然而双方的成效都非常有限。可并行的编程语言需要程序员有并行的编程思想，然而这多多少少有违人类本身的逻辑思维方式。同时，并行语言为程序调试带来很大挑战。使得大规模的并行程序开发变得相当困难。与此同时，编译器能在程序中找到的可并行部分也相当有限，这也使

得自动并行化的效率非常低。

研发多核芯片真的是一个好的决定吗？程序的并行极限又在哪里呢？要解释这个问题，我们便不得不提到计算机科学界的另一个经验法则——阿姆达尔定律。

阿姆达尔定律于1967年由IBM360系列机的主要设计者阿姆达尔首先提出。它代表了处理器并行运算之后效率提升的能力。该定律首先将一个程序分成可并行和不可并行两部分，并指出程序中对某一部分进行并行后所能获得的系统性能改进程度，取决于并行部分被使用的频率，或所占总执行时间的比例。

换句话说，在并行计算中用多核处理器对单个程序的加速受限于该程序所需的串行时间百分比。例如，一个程序中如果有一半是不能被并行的，那么即便是有无限核数的处理器，该程序能得到的最大加速比也只是两倍。

阿姆达尔定律给出了下面这个核心公式：$\text{speedup}=1/(s+(1-s)/n)$。该公式计算了一个程序并行化之后所能带来的最大加速比。其中，s 为程序串行部分（或不可并行部分）所占比例；$1-s$ 为程序可并行部分所占比例；n 为并行处理节点的个数，可以大致理解为处理器的核数。所以，如果一整个程序都是可并行的（$s=0$），那么能得到的加速比上限就是 n。

相反如果一整个程序都是不可并行的（$s=1$），那么加速比上限就是1。阿姆达尔定律通过该公式指出了多核的有效利用率和程序的可并行部分所占的百分比是密切相关的。这就像如果地主家的田地是很窄很长的；一次只能通过一个人的，那么就算雇来再多的长工也无济于事。

阿姆达尔定律的结论给并行化研究的领域蒙上一层令人沮丧的阴影，使得该领域像是一个一眼就能看到天花板的研究。在阿姆达尔定律中使用了两个设定作为前提，正是这两个设定让人们在1988年看到了对并行化研究不一样的前景。

阿姆达尔定律的第一个假设是固定负载（即计算总量不变）的量化标准。也就是说，它没有考虑硬件发展带动下的软件更新。举个简单的例子，20世纪90年代时人们用Intel奔腾处理器装 Windows 95操作系统；而到如今我们装有i9处理器的计算机不会再装 Windows 95了。换句话说，长工的技能提高的同时，地主的田地也在扩张。到了20世

纪 80 年代，Sandia 国家实验室的科学家们在使用 1024 个处理器时观察到 3 个实际应用程序随着处理器的增加发生线性加速的现象。于是在阿姆达尔定律的基础上，古斯塔夫森定律由此诞生。

古斯塔夫森定律于 1988 年由古斯塔夫森提出。古斯塔夫森指出，阿姆达尔定律的问题出在它的前提过于理想化。硬件性能的提升会直接导致软件规模及复杂度提升。即使算法仍然存在串行部分，但由于程序规模的不断扩大，算法中串行部分所占比例往往会持续减少。至此，他给出另外一个公式：$\text{speedup} = s + (1-s)n$，其中 s 是给定任务中不可并行的时间占实际执行时间的百分比，n 代表并行计算节点的个数。并指出在许多实际的应用程序中，因处理器核数的持续增加而得到接近线性的加速效果是可能的。

同古斯塔夫森定律一样，阿姆达尔定律的另一个设定是假设程序中可并行的部分在实际情况中可以完全被并行。这种设定作为一个纯数学模型忽略了可并行化在执行的时候所带来的开销。于是，费舍尔于 1988 年发表论文 *Your Favorite Parallel Algorithms Might Not Be as Fast as You Think*，并提出这样一个理论。如果一个输入大小为 n 的程序在串行时需要 $T(n)$ 个步骤来完成，那么该程序被 d 个计算节点(可粗略看作处理器核数)并行之后所需的执行步骤数会以 $\sqrt[n+1]{T(n)}$ 增加。

这个结论将逻辑门以及铜线连接的延迟考虑进去，打破了古斯塔夫森定律中线性加速效果的可能，并将可并行化的加速上限设在了一个更现实的高度。同时，在铜线延迟开始超过逻辑门延迟的如今，信号已然无法在一个时钟周期内被传达到芯片的所有地方。这也同样在并行处理的过程中加入了串行依赖。

正如之前所介绍的，科学家们试图以各种新科技突破现有的物理极限，但并行化领域里我们现在所能达到的离阿姆达尔提出的极限还很远。多数科学家们还在试图用各种方法去接近阿姆达尔定律所提出的极限。碳纳米管场效应晶体管的出现大大地改善了内部连接的延迟。Intel 公司在 2013 年声称其打算用硅光产品代替原有的铜线来连接芯片中的不同核。

当然，研究领域里也不乏试图再次突破现有体系所带来的物理极限的尝试。其中最大的项目要数对量子计算机的研究。从底层电路到计算机体系结构，再到上层的算法设

计，学术界和产业界都投入了大量的精力进行研究。

然而，虽然对于某些应用，量子计算机确实在理论上会优于传统计算机，但现阶段量子计算机的整个容错系统会带来巨大的开销，从而大大地抵消了其在理论上能够带来的优势。加之量子计算机从本质上来讲也是一个图灵机，其程序本身的复杂程度使得即便是量子计算机也很难超越费舍尔提出的并行化加速上限。

虽然从阿姆达尔定律提出之后并行化的研究屡遭质疑，多核技术的出现与流行对计算机体系结构、算法及程序设计都带来了重要的影响和新的挑战。未来这些方面都需要去适应多核芯片的发展。并行化的研究面临着诸多机遇和挑战，但相信未来会有更大的突破。

8.1.4　量子计算机：误解带来的乐观与恐慌

我们从工程、功耗、时空概念及复杂理论几个方面讨论了计算机的极限以及面对这些极限科学家们所采取的措施。下面我们将跳出传统计算机的领域（见图 8-2），从新兴科技的角度入手，通过对其极限的讨论，打破多年来人们对它们的误解。

图 8-2　跳出传统计算机的领域

基于前面所说到的传统计算机所面临的极限，当下计算机的研究越来越多地跳出了传统计算机的范畴。其中最热门的莫过于量子计算机。

对量子计算机的热捧让我们觉得量子计算机即将通过强大的计算能力取代传统计算机，并解决所有之前传统计算机无法解决的问题。普通用户渐渐地有了拥有一台量子计

算机的愿望。而传统计算机的架构师们渐渐地对量子计算机心生恐慌，害怕量子计算机的横空出世让自己多年的研究变得一文不值。

然而这项科技的发展真会给这个社会带来翻天覆地的变化吗？用一句话来总结：既有真实的发展，也有舆论的泡沫。那我们就来看看量子计算机是如何影响传统计算机的发展。

量子计算这一概念在1969年被威斯纳首先提出，并将其列入了他1983年发表的论文中。论文发表的前一年，费曼在一次公开演讲中也提出了利用量子体系实现通用计算的想法，而这一想法在1985年杜斯提出的量子图灵机模型中首次得到了实现。

当时人们研究量子计算机的初衷是为了模拟量子现象，服务于物理学。当使用计算机模拟量子现象时，由于庞大的希尔伯特空间所带来的庞大数据分析使得一次模拟所需运算时间变得相当长，甚至科学家可能穷其一生也看不到一次完整的结果。于是量子计算机的研究应运而生。

量子计算因其叠加和纠缠的特性对传统计算做了极大扩充。量子计算机对每一个叠加分量实现的变换相当于一种经典计算，所有这些传统计算同时完成，并按一定的概率振幅叠加起来，给出量子计算机的输出结果，这种计算称为量子并行计算。

从20世纪80年代的以理论推导为主的研究，到20世纪90年代Shor提出量子质因式分解算法；再到D-Wave公司发布的D-Wave One量子模拟器；再到如今Google、IBM公司从上层编程语言到底层电路设计的一整套对通用量子计算机研究成果，量子计算机的研究可谓是飞速发展。

然而人们对其技术本身的理解，在媒体的夸大下给人们一种量子计算机将无所不能的印象。《经济学人》杂志在2007年2月15日的期刊里曾说道：“量子计算机将通过并行处理所有可能性的方式在理论上可以有效解决NPC集合的问题。”

D-Wave公司在2009年时发布其制造了128量子比特的量子计算机的大新闻，很快受到业界的反驳与指责。就连2017年中国制造的光量子计算机在发布后也受到了褒贬不一的评论。那么量子计算机的极限到底在哪里呢？下面将从有效计算和计算能力两个方面来讨论。

我们先来看量子计算机能够有效(在多项式级时间里)解决怎样的问题。图灵把所有问题分成了可判定和不可判定两种,而图灵机只考虑可判定的问题集合。我们把可判定的问题集合按照其复杂度分成了P类、NP类和NPC类的问题。这些问题的关系可由图8-3表示。

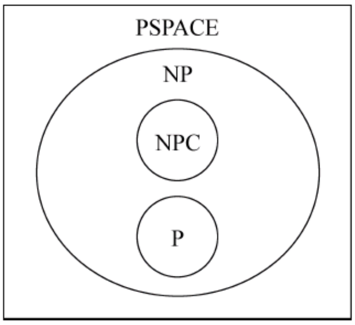


图8-3　复杂度问题的分类

其中,PSPACE是所有的决策问题的集合,指传统计算机可以用多项式级复杂度的内存通过非多项式级复杂度的时间解决的问题集合(包括象棋对弈等)。

P类问题是现在能用传统计算机有效解决的问题。例如,测试一个数是否是质数,或冒泡排序等。注意笔者所说的有效解决是指在多项式级时间内解决,并不代表传统计算机只能解决该类问题。实际上作为图灵机,传统计算机可以解决所有的可判定问题(即PSPACE集合内所有的问题),只是所需时间的长短不同罢了。

再说NP问题的概念,NP问题不是非P类问题。NP问题是指可以在多项式的时间里验证一个解的问题。或者说是在多项式的时间里猜出一个解的问题。至于NPC问题就是在研究NP问题的过程中找出一类非常特殊的问题叫作NP-完全问题。C是英文单词“完全”的第一个字母。NPC问题的定义非常简单,同时满足下面两个条件的问题就是NPC问题。首先,它得是一个NP问题;然后,所有的问题都可以约化到它。

约化的标准概念是:如果找到这样一个变化法则,对任意一个程序A的输入,都按这个法则变化成程度B的输入,使两程序的输出相同,那么我们说,问题A可约化为问题B。

那么媒体所说的用量子计算机有效解决NPC问题是否可行呢?答案是否定的。其实时至今日,计算机科学家们能找到的通过量子计算的特点将NP类问题转化为P类问题的算法也是寥寥无几,而其中最常见的就是阶乘的计算。

也就是说,能利用量子计算特性来有效解决传统计算机无法有效解决的程序其实并不多。在量子计算机只能有效解决少数NP问题的当下,NPC问题并不能靠量子计算机得到有效的解决。

原因很简单,因为该类问题其实是一个黑匣子,而人们只能通过猜答案并验证的方式

来得到结果（而非对其进行直接计算）。举个例子，如果一个问题有 s 种可能的答案，s 的大小随着问题输入的大小指数级增长。我们在运气好的情况下能一次猜中答案，而在最坏情况下需要试 s 次之后得到答案。也就是说，传统计算机需要平均 $s/2$ 次试错来解决这类问题。

现在把这类问题放到量子计算机上来。Lov Grover 在 1996 年的论文中找出了用量子计算通过 $\sqrt{s}$ 步来获得该类问题答案的算法。从 $s/2$ 次到 $\sqrt{s}$ 次的试错在很多情况下确实会带来客观的速度提升。例如，在 100 万可能性中，可以从之前的平均 50 万次试错减少到 1000 次，但即便是 $\sqrt{s}$ 也只是较简单的指数级复杂度，并非是多项式级的复杂度（因为 s 仍然会随着问题输入的大小指数级增长）。

早在 2002 年，Scott Aaronson 就指出该类问题如果用上述黑匣子试错的方式解决，即便是量子计算机也无法在多项式级复杂度的时间里解决。正如上面文章中提到的，解决 NPC 类的算法是否存在到现在仍未得到证实，但可以肯定的是，只用量子计算机的特性是无法有效解决这类问题的。于是 Scott Aaronson 在现有的复杂度理论上提出了一个新的集合，并命名为 BQP 类问题（Bounded-error，Quantum，Polynomial）。

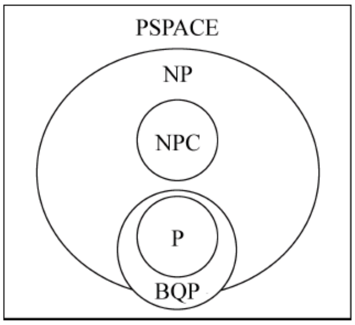


图 8-4　量子计算机能解决的 BQP 类问题

如图 8-4 所示，BQP 类问题包含所有 P 类问题和少数 NP 类问题，值得注意的是，BQP 类的问题包含一些非 NP 类的问题。也就是说，有那么一些问题用量子计算机解决所花费的时间会比传统计算机验证该类问题所花费的时间更少。但无论如何，解决 BQP 类问题，就是量子计算机所能达到的极限。支持 P≠NP 结论的计算机科学家们同样抱持着量子计算机无法解决 NPC 类问题的态度。

1998 年，Daniel Abrams 在论文中提到，如果在量子力学的公式中加入一项非线性的特性，量子算计机就能有效地解决 NPC 类的问题。但如果加入的这一项非线性特征成立，那么海森伯的不确定性原理将就此被推翻，信息传输也将突破光速的限制。正如

Daniel Abrams 在文中提到，这一特性恐怕只能用来理解为什么量子力学无法存在非线性特性了。换言之，这个理论也从旁佐证了量子计算机解决 NPC 类问题的不可行性。

值得注意的是，虽然 BQP 类问题包含了所有 P 类问题，也就是说，传统计算机能解决的问题量子计算机都能解决，但这并不代表量子计算机在所有程序的运行都能快过传统计算机。只有适合用量子算法的问题才能使量子计算机的运行速度超过传统计算机。

即使是最乐观的计算机科学家也认为，量子计算机不会完全取代现在的计算机。对于许多问题，使用量子计算机并没有太大的优势，例如，没有必要使用量子计算机去做文字处理，查邮件或者玩手机游戏。美国麻省理工学院（MIT）量子计算科学家 Aaronson 在 2008 年量子计算的局限性一文中分析了量子计算机对某些困难问题，例如，NP 中著名的“旅行推销员问题”，只能提供非常有限的加速。其中，NP 是指非确定性多项式。旅行推销员问题是指给定一系列城市和每对城市之间的距离，求解访问每一座城市一次并回到起始城市的最短回路。它是组合优化中的一个 NP 困难问题，在运筹学和理论计算机科学中非常重要。

量子计算的局限性如图 8-5 所示。

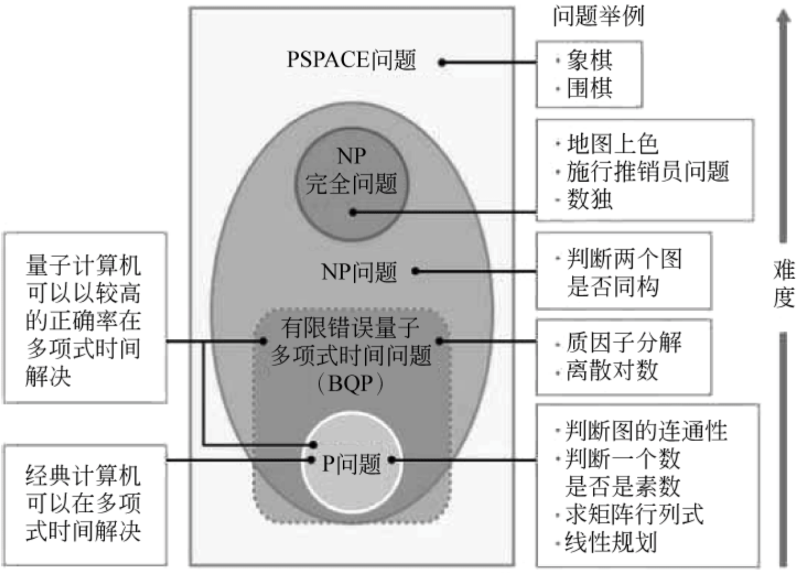

问题举例
PSPACE问题
·象棋
·围棋
NP
完全问题
·地图上色
·施行推销员问题
·数独
NP问题
·判断两个图
是否同构
量子计算机
可以以较高
的正确率在
多项式时间
解决
有限错误量子
多项式时间问题
（BQP）
·质因子分解
·离散对数
经典计算机
可以在多项
式时间解决
P问题
·判断图的连通性
·判断一个数
是否是素数
·求矩阵行列式
·线性规划
难
度

图 8-5 量子计算的局限性

上面从计算的有效性及计算能力两个方面讨论了量子计算机的极限。总结来说，从计算有效性来看，量子计算机能够有效解决一些传统计算机无法有效解决的问题，比如阶层的计算。但目前已知可归纳到这一类的问题并不多。而从计算能力来看，量子计算机的本质和图灵机并无差别，并不能解决不可判定的问题。一切对新兴科技过度的乐观和不必要的恐慌都来自于对其本身的误解。当然量子计算机的极限并没有阻止科学家们对NPC问题的探究，如果计算机理论暂时无法解决这些复杂度的问题，希望物理学界能在未来的某一天对这些问题做出结论。

8.2 量子计算机赋予计算机一种新的计算能力水平

随着电子计算机技术的飞速发展，计算机的运算速度和存储器容量以难以想象的速度飞快提高。计算表明，当存储器容量达到1024Mb时计算机内部电路的线宽只有0.1μm。这个线度被认为是集成电路的线度极限。因为电路线度小于0.1μm时，电路内运动的电子会出现量子效应。原来的电路理论不再适应了，取而代之的是微观粒子的量子理论。

利用量子理论设计的电子元件是量子元件。利用量子元件和量子算法设计的计算机称为量子计算机。理论研究和实验技术的发展为量子计算机的研制提供了可能。

8.2.1 我们为什么需要量子计算

从基因定位到太空探索，人类活动带来越来越多的数据。这些海量数据的处理已经远远超过经典计算机的能力范围。基于这种情况，在挖掘大数据潜在价值的过程中，量子计算将扮演重要角色。

1. 量子计算和大数据

量子计算的发展与现代计算机在本质上是相近的，都依赖于硬件、算法、操作系统、应用软件、云端平台的演进，进而孵化出一个萌芽中的量子计算产业生态。与传统计算相比，错误对量子计算的影响更大，所以，对于量子计算机来说很重要的一点是要解决容

错性。

量子计算的整体架构如图 8-6 所示。

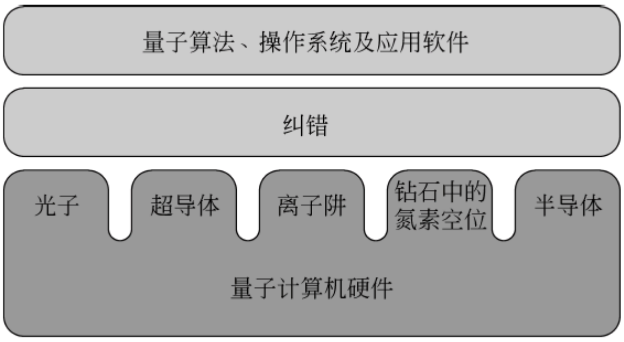


图 8-6　量子计算的整体架构

发展量子计算技术的主要挑战在于需要通过发展高精度、高效率的量子态制备与相互作用控制技术，实现规模化量子比特的相干操纵。在实验上，近年来科学家们已经在离子阱、超导系统、光子、钻石中的氮素空位和半导体等几个物理系统中实现了基本量子逻辑门操作和少数量子比特的简单量子计算。不过，因为对物理系统性质的要求常常互相矛盾，所以建造有规模、有实际应用价值的量子计算机还存在巨大的技术困难。

在构建量子计算机的理论和实验研究中，以牛津大学研究为代表的离子阱量子计算机在所有实现基本量子比特操作（存储器、状态输入、状态读出、逻辑门）的性能表现维度上，目前被认为是量子计算机物理实现最成熟、最有希望的方案。超导电路与离子阱的发展水平旗鼓相当。

未来两到三年内，量子计算机有望扩大到 50 量子比特，达到所谓的“量子优越性”。也就是说，在某些问题上，量子计算机的计算能力将超过目前最强大的经典并行计算机。但要达到真正的商业应用，量子比特需要达到百万级，这是一个非常大的门槛，当规模如此庞大时，量子计算机就可以克服错误问题。

目前已经知道，量子计算机至少在解决某些类问题上，如分解大数质因子、随机数据库搜索等，相对经典计算机来说，具有大规模加速作用。量子计算未来主要会应用在复杂的大规模数据处理与计算难题，以及基于量子加密的网络安全服务。例如，环境监测领域

的气象预报；医学领域的基因测序与药物研发；金融领域的投资大数据分析、预测与风险建模；网络安全与即时通信领域的量子加密，以及为人工智能提供强大的计算能力。

2. 人工智能和机器学习

像人类一样，量子计算机也可以从经验中学习，进行自我纠错。例如，量子计算机可以修改出现乱码的程序代码。这一概念被称为量子计算机的机器学习——与 Facebook 新闻流根据用户的“点赞”而进行个性化的推送相类似，只是更为复杂。

量子计算机的机器学习可以帮助人们更快、更高效地做很多事情，具体应用场景包括人脸识别、图像理解、音频语音理解、用户画像、机器人和自动驾驶车的图像识别及决策等。用量子算法，可以更快地构建机器学习模型，对于数据越多的问题，节省的时间就越多。

例如卫星，它在运行过程中收集了大量的图像和视频资料，产生海量数据。人们不可能精细搜索和分析如此多的数据，但是这样却可能会错过许多关键信息。量子计算机可以比经典计算机更快地筛选海量数据，并指出哪些图像和视频我们应该做进一步分析，哪些则可以忽略。经过数以万计的统计，我们发现经典计算机并不擅长从海量图片中迅速完成“孙悟空在哪儿”的识别任务，但量子计算机却非常擅长从混乱的背景中找出具体人物或者细节。例如，Google 公司将在无人驾驶车中用量子计算机区分汽车和景物。

3. 信息安全

现有加密系统受到量子计算机威胁。但是通过使用量子力学特性，加密技术将变得更加安全。这种超级安全通信被称为“量子密钥分配”，它允许某人发送信息给其他人，而只有使用量子密钥解密后才能阅读信息。如果第三方拦截到密钥，鉴于量子力学的原理，信息会变得毫无用处，也没人能够再读取它。

量子加密通信已经在全球开始使用。例如，一个名为 ID Quantique 的瑞士量子加密公司在荷兰电信公司 KPN 的数据中心，以及瑞士的金融机构之间，建立了量子连接；2015 年，日本东芝研究院将量子加密的基因组数据从仙台的研究机构发送至 7km 以外的东北大学；2016 年，英国电信公司 BT 和日本东芝在 BT 的 Ipswich 研发中心联合举办了英国首个安全量子通信展示会。

后量子密码学则致力于创建出即使是未来的量子计算机也无法破解的密码。PQCRYPTO是一个受欧盟资助为期三年的项目，专注于开发后量子加密。2016年，PQCRYPTO的一些研究成果已经被Google公司用在了Chrome浏览器运行的后量子加密测试中。而在斯诺登事件后，美国国家安全局于2015年表示将更新其所有的加密技术，使它们无法被量子计算机破解。

4. 最优化问题

许多证据表明量子计算机比经典计算机更适合进行某些需要挑选出最优化解决方案的任务，而大量的商业活动都依赖于最优化方案。例如，在开始制造汽车、飞机部件前，人们可以运用计算机模型优化汽车和飞机的设计方案。飞机机翼设计是一个特别复杂的情况，量子计算机则可以提供更有效的设计而形成最佳的制造方案。许多飞机制造商都很重视量子计算机带来的变革。

从2013年秋季量子计算机开始运行以来，NASA的研究人员就一直在使用它来研究空中交通管制，包括自主性、机器人、导航和通信、系统诊断、模式识别、异常检测、任务规划和调度等领域的优化问题。通过这些研究，NASA量子人工智能实验室希望能证明大规模的量子计算机，能比采取了最佳优化算法的经典计算机更快地解决具体问题。例如，Google公司在量子计算机D-Wave 2X上优化一个含有大量变量的函数，比在经典计算机上快一亿倍。

我们可以自定义什么样的问题需要找出最优化解决方案，例如，产品收入最大化、点击转化率最大化、用户满意度最大化、成本耗时最小化。某些人工智能问题也可以转化为优化问题，例如，构建预测模型，使其对未来数据的预测误差最小。

举例来说，马车和汽车代表的不仅仅只是速度不同，更是商业生态以及社会生态的不同。量子计算就像是新的“引擎”，代表了新的商业形态和社会形态。蒸汽机的到来引发了第一次工业革命；燃气机的使用引发了第二次工业革命；计算机的诞生引发了第三次工业革命；那么量子计算机的到来，很可能会推动第四次工业革命的构想正在变成实现。

量子计算机一旦投入使用，许多行业可能将会受到颠覆性的影响，目前很多看似不可能有太多突破的领域未来都会有很大的改变。量子计算机在各行业的应用机会如图8-7

所示。

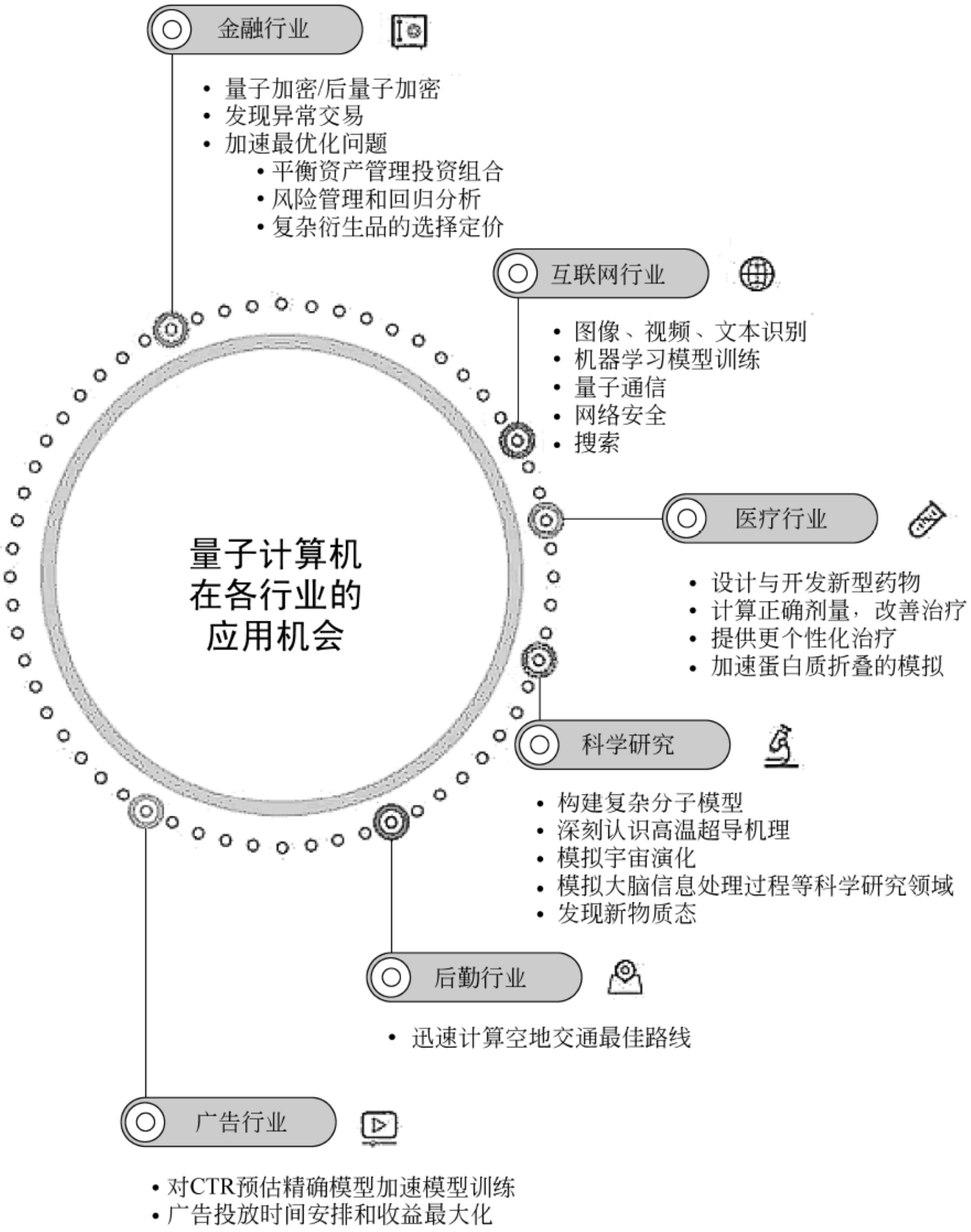

金融行业
• 量子加密/后量子加密
• 发现异常交易
• 加速最优化问题
• 平衡资产管理投资组合
• 风险管理和回归分析
• 复杂衍生品的选择定价
互联网行业
• 图像、视频、文本识别
• 机器学习模型训练
• 量子通信
• 网络安全
• 搜索
医疗行业
• 设计与开发新型药物
• 计算正确剂量，改善治疗
• 提供更个性化治疗
• 加速蛋白质折叠的模拟
科学研究
• 构建复杂分子模型
• 深刻认识高温超导机理
• 模拟宇宙演化
• 模拟大脑信息处理过程等科学研究领域
• 发现新物质态
后勤行业
• 迅速计算空地交通最佳路线
广告行业
• 对CTR预估精确模型加速模型训练
• 广告投放时间安排和收益最大化
量子计算机
在各行业的
应用机会

图 8-7　量子计算机在各行业的应用机会

8.2.2　量子计算机要从囚禁原子开始

量子计算机是一种遵循量子力学规律，进行高速运算、存储及处理量子信息的物理装置，其运行的是量子算法，处理速度惊人，比传统计算机快数十亿倍。

量子计算机本身处理的是量子数据，那么要实现超强的功能就需要有量子。我们要把原子量子化，那么便需要从囚禁原子开始。囚禁原子是原子物理学的一种新的实验平台，研究人员可以用此方法自由操纵单个原子，此步骤完成后，就可以开始冷却原子。可以说囚禁原子是量子计算机的通用方案。

在原子被“囚禁”后，就需要降低原子的温度，一般超冷原子的温度需要接近绝对零度。因为原子在常温下的速度高达数百米每秒，只有让原子保持在极低温度状态，才可受控制。图8-8中系统是模拟凝聚态物质中的量子现象，如高温超导等。该系统主要用于操控原子的量子态，冷却原子后就可以开始这一动作。不过，如何保持长时间的量子态是最大的技术瓶颈。

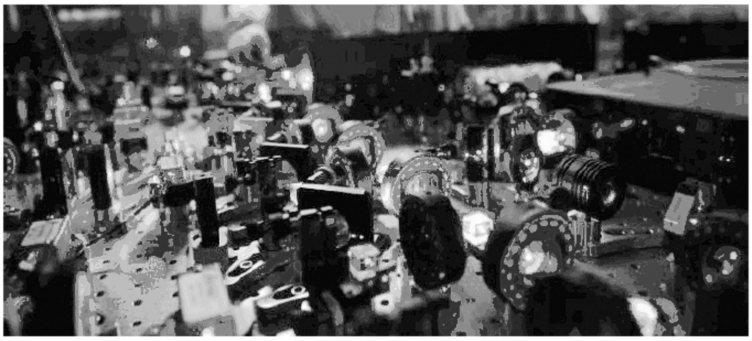


图8-8　制备并研究极低温分子

此外，量子计算机还致力于控制分子的状态，分子在常温下会做不规则的热运动，温度越低分子运动得越慢，在低温情况下更易受控制，进一步进入量子态。

超低温状态下的原子状态如图8-9所示。

一般情况下，超冷原子的温度接近绝对零度，在此情况下就可以进入量子态。

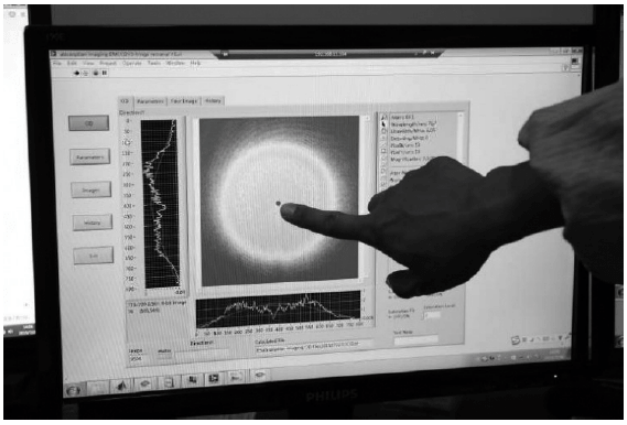


图 8-9　超低温状态下的原子状态

8.2.3　必须“冷酷”的量子计算机

量子计算是一门理论科学。它是研究如何直接应用量子力学现象(例如,量子叠加态和量子纠缠态)对数据进行操作的计算系统的科学。在最终的运算结果上,量子计算机和现有计算机没有任何不同(否则一定是有一方算错了,那算错的一方也就没有什么实用价值了)。它们最大的不同之处在于运算的过程有着天壤之别,后文将会详细解释。

量子计算模型主要有 3 种。

(1) 量子电路模型。

(2) 单向量子计算模型。

(3) 绝热量子计算模型。

1. 量子电路模型

量子电路模型是把量子计算过程化成像经典计算一样有不同的逻辑门作用在量子态上,最后得到所期待的量子态。

2. 单向量子计算模型

单向量子计算模型是把量子计算,化成通过传输和测量二维簇态,使得我们可以得到想要的量子门操作。

3. 绝热量子计算模型

绝热量子计算模型是通过先把问题划归成复杂的汉密尔顿量的基态的问题（即找到基态就可以找到最终结果），然后开始与一个简单的汉密尔顿量，通过绝热过程最后得到所需要的基态。

1）量子计算的终极实现

量子计算研究的终极目标之一是制造并应用通用量子计算机。以当前的设计构想，至少要能够处理上百量子比特位才有意义。硬件上的具体物理实现有很多，比如通过光子学、核磁共振、QED腔、量子点、里德伯原子、离子阱、约瑟夫森结等来实现。量子计算研究科研框架如图8-10所示。

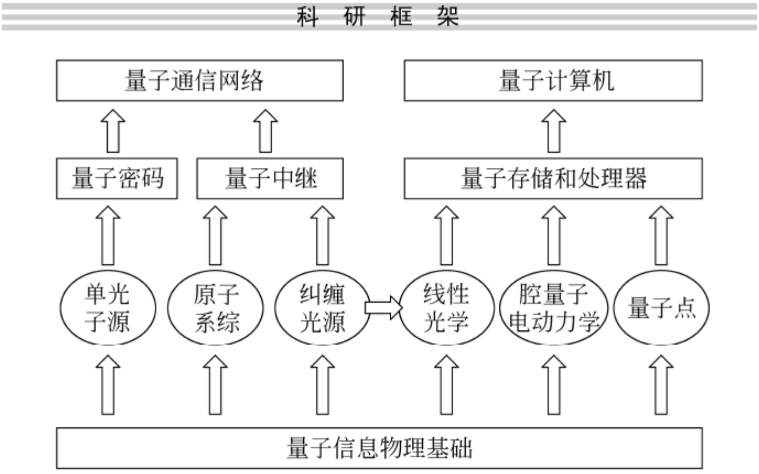

科研框架
量子通信网络
量子计算机
量子密码
量子中继
量子存储和处理器
单光子源
原子系综
纠缠光源
线性光学
腔量子电动力学
量子点
量子信息物理基础

图8-10　量子计算研究科研框架

其中，在量子信息物理的基础上，发展成为两个方面的技术应用。

第一个方向：通过单光子源的研究，进入量子密码领域。通过原子系综和纠缠光源的研究，进入量子中继领域。通过量子密码领域和量子中继领域技术的合成，发展成为量子通信网络应用技术。

第二个方向：通过线性光学、量子点和腔量子电动力学的研究，进入量子存储和处理器领域。进一步发展成为量子计算机应用技术。

较之 D-Wave 量子计算机，比较出名的 D-Wave 1 代和 2 代使用的都是约瑟夫森结。NASA、CIA、Google 公司都购买了 D-Wave 进行相关研究。D-Wave 受到质疑的地方在于其应用场景受限，目前的设计并不是通用量子计算机。

IBM 公司正在研发的是基于量子逻辑门的通用型量子计算机，所以通用性没有问题，所有的量子算法都能运行。此外，IBM 公司还完成了两个很重要的突破。

(1) 同时检测两种量子误差：bit-flip 和 phase-flip。从而大大增强了量子计算机的稳定性。之前的研究只能测量两个错误中的一个，也就无法做到错误纠正。如今 IBM 公司解决了这个问题。

(2) IBM 公司提供了有史以来最好的可扩展性。当然，落实到实际硬件开发应该还会有新的问题。IBM 公司接下来的目标是把量子比特加到 50～100。再往后就需要更多的研发资源了。

在这里附带澄清一下很多媒体对量子比特的普遍误解，以及对量子计算的误解。对于量子计算的优势，媒体上常见的解释：相对于我们常用的电子计算机采用的 0、1 二进制值，量子计算机每一个量子比特都能存储 0～1 的信息。这是一个想当然的解释，这根本不是量子计算机的本质优势。很明显我们用电阻电容组成的模拟电路一样可以表征 0～1 的任何连续值。所以说本质区别不是比特所携带数值的无穷可能性，而是比特信息的量子叠加态特性。对于多比特的运算，量子计算机的优势才得以明显体现。所有的比特可以同时完成逻辑运算，这一点是传统电子计算机根本做不到的。

对于多比特的量子系统，整个系统的量子比特状态是可定量预测的，而单个量子比特是不能确定的。

2) 量子计算机的工作温度

理想情况下，量子计算不会有误差。但实际上由于环境噪声(主要是热和电磁辐射)，量子系统会受环境干扰。只有在零场强和绝对零度的环境里，才能有理想状态下的量子计算。现有量子计算技术中，一些前沿性研究需要将材料冷却到绝对零度左右，这阻碍了量子计算机从理论到实用的进程。

量子计算机的工作温度范围如图 8-11 所示。

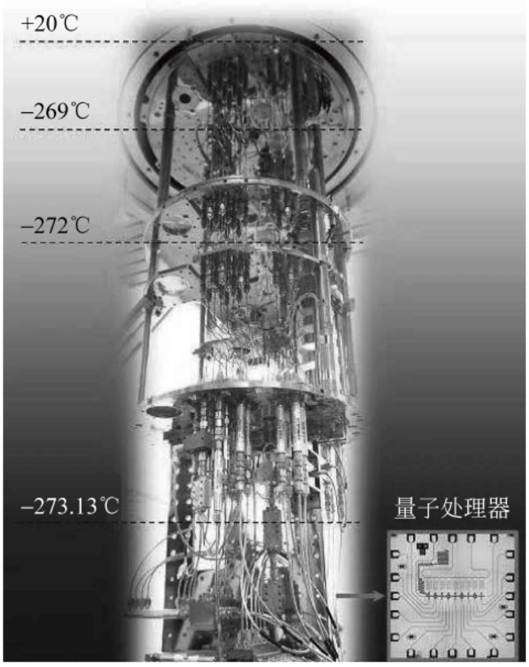


图 8-11　量子计算机的工作温度范围

如果一个量子计算机能够组建成 50 量子比特，当今世界前 500 名的超级计算机全部加起来，功能都无法胜过它。

3）两个突破性研究成果

IBM 公司的科学家在《自然通信》杂志上发表了两个突破性研究成果，第一次证明了能同时检测并测量两种类型量子错误，同时验证了一种新的正方形量子比特环设计是唯一能在更大维度上被扩展的物理结构。

科学家试图攻克量子计算机所面临的巨大难题之一，就是控制或者移除量子退相干——由于热、电磁辐射或材料缺陷引起的计算误差。广泛存在于量子机器中的两种类型量子错误——位翻转和相位翻转——一定会发生在任何真实量子计算机上。但到目前为止，科学界也只有单独解决一种类型量子错误的可能性。不过，解决两种类型的量子错误，恰恰是迈向量子纠错的关键一步，也是建立实用、可靠的大型量子计算机的关键需求。

IBM 公司创新的复杂量子比特电路是由 4 个超导量子比特组成的正方形芯片。“在

此之前，这一领域的工作使用线性排列，只能看着翻转错误提供出信息不完整状态的量子系统，而这种系统不足以构成实用的计算机。”IBM 公司量子计算团队主管杰伊・甘拜塔说，“我们的 4 比特正方形芯片，能带领我们同时检测两种类型量子错误，并可被扩展到更大的量子系统。”

（1）遇见量子比特。

今天的计算机都把数据存储在极微型的晶体管当中。每个晶体管可以容纳一个“比特”的信息：1 或 0。大约在 30 年前，科学家提出一种机器计算概念，它可以超越二进制系统，把数据存储在根据神奇的量子力学原理打造的系统当中。不仅是 0 或 1，一个“比特”信息有可能同时是粒子和波，同时存储，这就是叠加原理。

同样，两个比特可以同时容纳 4 个值：00、01、10 和 11。如果你继续添加量子比特，理论上就可以创建起一个比今天任何计算机都要强大的机器。

量子计算和量子算法的问题都是你将要如何利用它们，但这样的超级机器还不存在。现在看来，量子比特还是不稳定的东西。如果你试图观察量子系统的状态，它们会“散屑（使检波器恢复常态）”，陷入另一种状态，而且不再拥有 0 和 1，而是只有 0 或 1，就像今天的传统计算机。

要建造一个真正的量子计算机，研究人员必须抓住量子比特从一个状态散屑进入另一个相对的状态的机会。

（2）每次测试的结果都相同。

这样做的方法有很多，虽然没有真正攻克这个难题，但部分方法还是很有希望的。2015 年 4 月底，IBM 公司的研究人员完成了四量子比特原型电路，为推出真正的量子计算机奠定了基础。该电路采用四个超低温超导设备构建。检测两种类型量子错误的设备如图 8-12 所示。

测试结果显示如图 8-13 所示。

研究人员对 IBM 公司的这个新服务进行了试用，结果是这个系统相当稳定，每一次测试它几乎都得到了相同的结果。这在传统计算机中是个平常的现象，但在基本都是围绕捕获概率展开的量子计算机世界中，结果的稳定一致就意味着标志性的进步。

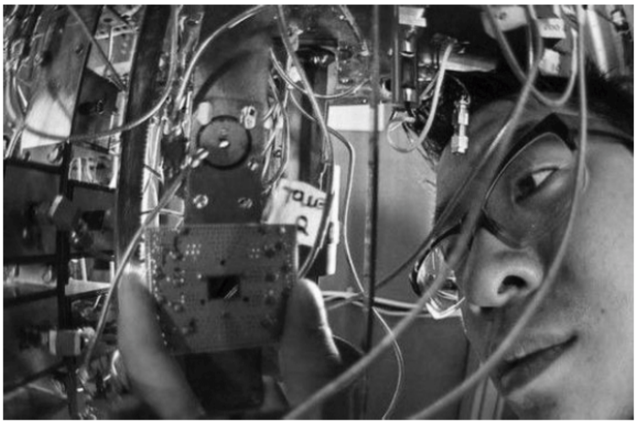
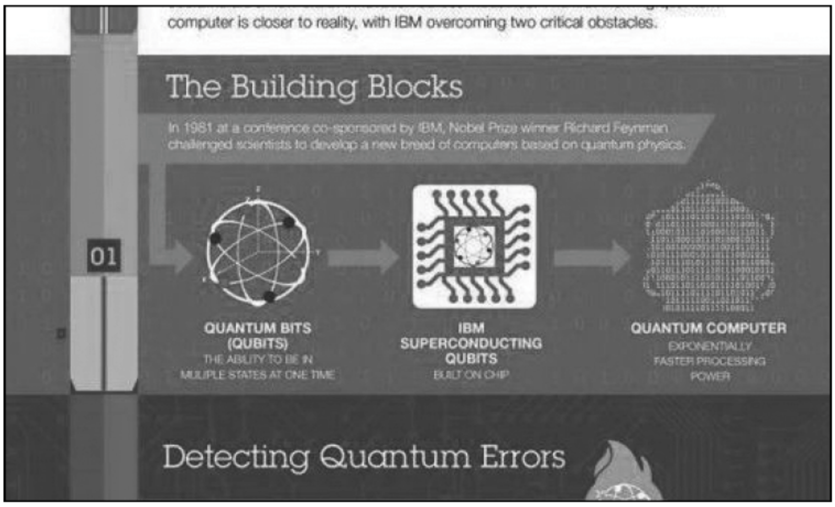


图 8-12　检测两种类型量子错误的设备



computer is closer to reality, with IBM overcoming two critical obstacles.

The Building Blocks

In 1981 at a conference co-sponsored by IBM, Nobel Prize winner Richard Feynman challenged scientists to develop a new breed of computers based on quantum physics.

01
QUANTUM BITS (QUBITS)
THE ABILITY TO BE IN MULIPLE STATES AT ONE TIME
IBM SUPERCONDUCTING QUBITS
BUILT ON CHIP
QUANTUM COMPUTER
EXPONENTIALLY FASTER PROCESSING POWER

Detecting Quantum Errors

图 8-13　测试结果

四量子比特原型电路如图 8-14 所示。

虽然目前已经对量子计算机的加密系统进行了广泛研究，但人们认为比较有实用价值的是量子系统，它能解决今天不能解决的物理和化学难题，可能在材料科学、药物设计等方面具有不可估量的潜力，能开发出一系列新的应用领域。例如，它能让科学家摆脱昂贵的实验室实验，加快设计出新的材料和药物成分，加速相关药物化合物的创新速度等。

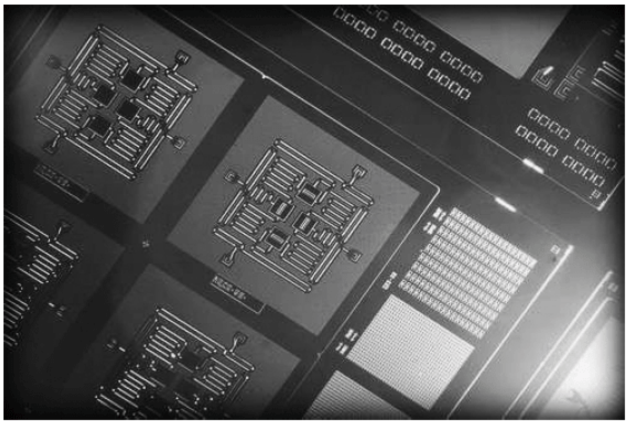


图 8-14　四量子比特原型电路

此外，量子计算机还可以快速处理更大规模的数据库，可以大规模处理多样化、非结构化的数据，这将改变人们进行决策的方式，并有助于研究人员跨行业做出全新研究成果。

8.2.4　量子计算机研制面临的技术困难

既然可供实用的量子计算机尚未问世，那就说明量子计算机的研制仍然面临某些尚未解决的困难。根据对近年来有关量子计算机研制资料的分析，可以看出量子计算机的研制目前面临的主要困难仍然是如何克服消相干，即量子纠错。

我们知道量子计算机的建立是以量子并行计算为基础。无论是量子并行计算还是进行量子模拟，其本质都是利用了量子相干性。失去了量子相干性，量子计算机的优越性就消失殆尽。但在实际量子计算机系统中，无论采用哪种量子体系作为工作机制，量子相干性都很难永久保持。相干性的衰减（即消相干）总是不可避免的。

为什么会形成消相干？其主要原因是系统和外界环境的相互作用。因为在量子计算机中，执行运算的量子比特不是一个孤立系统，它必然要与外部环境发生相互作用，这种作用实际上是对量子体系的一种微扰。这种微扰的长期存在可能引起量子体系状态的改变，破坏量子体系的相干性，即导致消相干。Uruh 定量分析了消相干的影响，结果表明，量子相干性的指数衰减是无法避免的，即消相干始终是存在的。

相干性的丢失会导致运算结果出错。除了消相干会导致量子错误外,其他一些技术原因,例如量子门操作中的失误等,也会导致量子错误。因此,问题的关键就是,在门操作和量子存储都有可能出错的前提下,如何进行可靠的量子运算?Shor 在此方面的一个重要贡献就是提出了量子纠错的思想。

这种纠错思想是经典纠错码的量子类比。经典纠错码采取的是冗余编码方案,即如果输入 1 比特信号 0,现在可将其编码为 3 比特信号 000。在存储中 3 比特中任一比特发生错误,如变成 001,则可以通过比较这 3 比特信号,按照少数服从多数的原则,找到出错的比特,并将其纠正到正确信号 000。Shor 提出的纠错的思想与这种思想相类似,但又有不同。

其原因之一是量子运算不再局限于两种状态 |0〉和|1〉,而是涉及二维态空间中的所有态,因此,量子错误出现的概率也就大得多。

其二是按照量子不可克隆定理,一个任意量子态是不可能进行复制的。

因此对一个单比特输入态|〉,无法将其编码为 3 比特输入态|〉|〉|〉。但 Shor 却给出了一个全新的编码方案,即利用 9 个量子比特来编码一比特信息,通过此编码,可纠正 9 比特中任一比特所有可能的量子错误。Shor 的量子纠错思想令人兴奋,因为它指出了量子纠错的可行途径。

在此基础上,各种量子纠错码接二连三地被提出。值得一提的是,作为 Shor 量子纠错思想的重要应用,利用相位一致性对信息进行筛选也是一种减少错误的方法。1998 年,美国麻省理工学院的专家们设法使一比特量子信息穿过液态丙氨酸分子或三氯乙烯分子的三个核子的自旋从而扩展了信息。因为被扩展后的信息很难被破坏,而且通过对扩展信息的研究可以获得量子态之间的纠缠关系。从而利用纠缠的性质作为一种分析量子信息的间接方法来研究状态之间的相互作用,避免了直接测量。这项技术使得人们有能力在一个量子比特的相位一致中发现并修复错误,为量子纠错提供了又一可行的途径。

8.25 量子计算机会不会取代今天的计算机

量子计算机会不会取代今天的计算机?这是我们的第一个问题。

现在学界的主流意见：在可见的未来，不会。

1. 量子计算机和传统电子计算机的共同繁荣

无论从现有的理论还是实际来看，在短期内量子计算机都不会完全取代现在的计算机。更可能的是两者共同繁荣。

学术界目前的主要研究方向也是这样，用量子计算机去运行特定的程序，在传统计算机欠完善的领域发挥作用了。

原因有两方面。

首先从量子算法理论来看。量子计算机需要特定的量子算法才能发挥出量子计算的强大威力。但是，并不是所有的计算都可以用量子算法加速。虽然量子算法绝不会比传统算法慢，但能像Shor算法和Grover算法那般完全超越传统算法的其实比较少见。不少问题上人们暂时都还没有得到很好的量子算法。不过，人工智能或机器学习里很核心的优化过程却很幸运地与量子计算是天作之合。这个将在后文提到。

再从实践来看。D-Wave这家量子计算机公司开发了世界第一款商业量子计算机。但实际上，这款量子计算机不是通用量子计算机，并不能运行所有的量子算法。D-Wave实际上是一台量子退火机。它的主要工作方式是调整伊辛模型的参数来构造满足某优化问题所对应的量子态，再用量子退火算法来求解。Google公司愿意花1000万美元买一台D-Wave，Quantum AI Lab就是看中了D-Wave在人工智能上的强大功能。目前512量子比特量子计算机所模拟的最复杂的人工智能问题都能在1s左右解决。

通用量子计算机是一个超出目前科技水平太多的技术。以至于大多数科学家更愿意研究具有特定量子结构的量子计算机，用来执行特定的量子计算功能。例如，Google公司有一项量子计算需求，就为此配一台能专门完成这项量子计算的量子计算机，其他部分再交给电子计算机分工处理就可。

想一想量子退火机尚且要在20mk的温度下才能运行。通用量子计算机的制造复杂、精密且昂贵，而且至今没有好的方案去实现。量子点、核磁共振、量子光路、超导环等所有可能的途径都有科学家在研究。这个研究主要针对的是量子计算机目前的缺陷。

因为制造通用量子计算机困难很多，所以量子计算机很难全面取代传统计算机，但是

量子算法相比经典算法有天然的优势。

2.量子算法的上限和潜力远高于经典算法

一方面，就是因为0和1可以被一量子比特同时存储，一量子比特需要用两个数描述其叠加态。N量子比特可以存储2^N个数，算一算2^N可以是N的多少倍。如果未来出现一台量子计算机的算力超过地球上所有经典计算机之和一定不要觉得奇怪。

另一方面，量子计算机是可逆计算机。这是许多人会忽略的一点。经典计算机则是不可逆计算机。不可逆计算过程每一个比特的操作都会有热损耗。集成度越高，散热越困难。摩尔定律会在7nm左右时失效，最多还有十年，这是业界的普遍观点。

摩尔定律失效后，提高计算能力只能靠堆积核。这种靠堆积带来的计算能力上限也很低，能耗又高，又不能小型化。如果想突破经典计算机的极限，人们必须要攻克量子计算机这个难题。

量子计算机意味着无能耗。能做多小做多小。一个计算能力超过经典计算机之和的量子计算机只需要一颗纽扣电池就能驱动理论上也是可行的。一块手表的计算能力甚至可以超过超级计算机，而且只需要一块纽扣电池就能驱动它了。这是因为，量子逻辑门操作全部是可逆变换，整个过程不产生热量。理论上，耗能可以降到极低。

但是，当数据太大时，Google之类的企业会很愿意使用具有特定量子功能的机器。笔者预测现在需要超级计算机的地方，会成为未来量子计算机首先投入使用的地方。

虽然有种种困难，但是大家普遍认为量子计算很快就能在人工智能领域发挥作用。因为量子退火机D-Wave可以在人工智能领域完全地发挥出量子计算功能。这也是Google公司建立Quantum AI Lab的主要原因。

在自然科学领域，量子计算可以很高效地模拟诸多自然过程，会成为相关领域科学家的一大利器。所以，用量子计算机模拟自然现象有着巨大的吸引力。

还有一点很重要，基于量子逻辑门的标准量子计算与绝热量子计算是等价的。人们可能不需要按照传统计算机一样做出逻辑门就能进行量子计算。

量子退火就是绝热量子计算过程——制备量子态，等其绝热演化到基态，基态直接就能给出计算结果。想一想这是多么恐怖的计算能力，大自然本身就是绝佳量子计算机。

自然演化就是计算结果。这种绝热量子计算方式甚至不需要人们构建量子逻辑门。

所以，D-Wave 也有可能在未来被改进成能顺利执行所有量子计算功能的通用型量子计算机。这给人们带来了新的曙光。

8.2.6 量子计算机最终什么时候实现

围绕这一话题，有乐观派也有悲观派，笔者仅在此分享几个个人观点，希望能帮助读者进一步认识量子计算，期待更多学者加入到这个“满足好奇心又有用”的研究领域，推动量子计算机的早日实现。

1. 量子计算机是传统计算机的有效补充

量子计算机不会是电子计算机的替代品，而是一种有效的补充。量子计算机不会是电子计算机的一种更快、更大或更小的版本，而会成为在电子计算机不能胜任的领域求解特殊问题的计算系统，是传统计算机的一种有效补充。

2010 年，莱德等人在《自然》上发表的一篇文章中，将量子计算机比作激光器。激光器诞生之前，灯泡等非相干光源已经广泛使用。作为一种相干光源，激光器诞生后并未替代灯泡用来照明，而是用到了工业、通信、科学、娱乐等人们工作和生活的方方面面，发挥了极大的作用。

传统电子计算机是一种“非相干计算”，而量子计算机恰是一种“相干计算”。量子计算机的发明也将像激光器那样，不会替代电子计算机，而是发挥甚至目前也无法预知的重要作用。

2. 量子计算是“最高境界”的量子信息技术

量子信息技术利用量子效应，为人类突破信息感知、传输和处理的经典极限提供了新的理论方法和技术途径。例如，量子通信中的量子密钥分发技术，利用测量坍缩和量子不可克隆定律等实现理论上的无条件安全；量子精密测量技术，利用量子纠缠等实现对经典测量极限的超越等。在这些技术中，量子计算的要求最高，其研究涵盖了很多其他量子信息技术的关键原理与方法。一旦量子计算技术取得突破，必将带动整个量子信息领域的全面发展。

比起标准的量子计算,非标准量子计算或量子模拟更有可能尽早实现。

标准量子计算(也被称为通用量子计算)采用线路模型,需要大量量子门的操控,实现难度大。事实上,费曼首次提出量子计算的概念时,旨在实现对量子物理过程的模拟,而这种量子模拟是经典计算机难以有效解决的。随着量子计算技术的不断突破,类似 D-Wave、玻色采样等非标准量子计算机或量子模拟机,更有可能尽早实现。

3.学科交叉将为量子计算研究注入新的活力

集成化和小型化成为构造大规模量子比特系统的主要发展方向,为量子计算技术的发展提供了重要途径。

量子点、超导等量子体系本身就属于固态量子计算方案,因其小型化的技术优势受到人们的广泛重视。光量子计算、离子阱量子计算等也正在向芯片化方向发展。这种集成化和小型化的研究给构造更大规模的量子比特系统提供了重要的技术途径,将是未来的研究重点。学科交叉将为量子计算研究注入新的活力,助其取得更大突破。

当我们在一个学科领域遇到难题时,也许在比它更大的领域能够寻找到答案。通过物理学、计算机科学等多个学科的交叉合作,量子计算研究一定能取得更大突破。

8.2.7 如果量子计算机被推广,我们会失业吗

“量子计算”的概念被炒得火热,很多计算机行业从业人员担心量子计算机会像内燃机取代蒸汽机一样,取代现有计算机领域的部分知识,间接导致具备某些技能的人才失业,事实真会如此吗?

如果有一天,量子计算机开始大规模推广,会不会导致现有的部分技能被淘汰呢?我们来看看在某知识社交平台部分网友的讨论。

网友 Lcici:

量子计算机的出现并不是为了取代计算机,因此不会出现上述问题。

那么,为什么要造量子计算机呢?学术界的大佬们经常会用下面这段话比喻:“量子计算机和经典计算机的对比,就好比激光器和电灯泡的对比一样,并不是内燃机和蒸汽机的关系。内燃机和蒸汽机本来就是为了解决同样的问题而诞生的,效率高的自然会取代

效率低的。而激光器和电灯泡的功能并不是一样的,二者在使用场景方面具有很大差异。”

简单地说,电灯泡就好比传统计算机,它有其自己的适应场景。量子计算机只是为了解决某些特定领域中,必须使用特定算法,传统计算机无法解决的复杂问题(比如Shor算法处理解密问题,模拟量子多体系统的演化)。

因此,目前程序员所学的技能并不会被量子计算机所取代。

网友飞龙:

算法及语言不会被完全推翻,量子计算机可以更好地解决性能问题。

(1) 追求效率的算法可能会被废除,而从无到有的算法不会被废除。或者说算法的优化可能会被废除,算法本身不会。

(2) 高级语言不会被推翻,而是直接编译到量子计算机的指令集。

(3) 量子计算机也需要向后兼容,现在这么多程序都是由电子计算机的某种指令构成,不可能完全重新编译。也就是说你还可以按照以前的知识来做东西。

(4) 由于量子计算机帮你解决了性能问题,产能会越来越重要。人们更熟悉已经学会的东西,会越来越依赖这部分东西。

网友九公子:

单说量子计算机太玄奥,可以把这个问题换成简单一点的提法。

(1) 如果计算机的运算能力一夜之间突然提升好几个数量级,会产生什么影响?

① 所有科学领域的发展都将极大提速,因为届时计算机模拟技术将成为诸多学科的首选。几年之内人类会取得大量的新科研成果,一年只颁发一次诺贝尔奖将被认为是愚蠢的。

② 共享计算将成为继共享单车后的下一个热门风险投资领域。毕竟大部分计算机会出现计算能力冗余的现象,不共享一下太浪费了。

③ 著名的摩尔定律退出历史舞台。整个计算机芯片产业会彻底洗牌,当然受到直接影响的可能是Intel公司,毕竟摩尔定律的别名是“Intel的年度工作计划”。

④ 密码不再安全了,因为破解密码的效率大幅提升。即使以传统计算机的计算能

力，在今天一个安全的密码也至少需要长度上达到16位左右。一旦量子计算推广，这一长度要求会增加好多倍，没有人愿意记住一个两百多位的密码，世界需要一种新的安全验证方案。比特币或将贬值。想象一下到时中国矿场的挖矿能力有多恐怖吧……

(2) 计算机不再基于二进制计算，会产生什么影响？

① 几乎所有的现有编程语言都不再适用。量子计算机的基础计算以集合为单位进行，传统计算机的基础计算以单个元素为单位。如果在量子计算机上强行继续沿用在二进制的理论基础上发展起来的传统编程语言，相当限制所有参与运算的集合里只包含一个元素，这无异于自我阉割了绝大部分计算能力。新式编程语言的雏形，或许出现在今天的ErLang这类被认为超前、边缘化的并发式语言里。

② 带宽和流量计算变成一个玄学问题。你家社区宽带的广告语：“上千叠加态美国大片光速秒看，永不正交，一次纠缠不到一毛钱。”

③ 冯·诺依曼的历史地位从现代计算机之父升格为计算机之神，毕竟这位科学家提出了冯·诺依曼架构，还写了一本书叫《量子力学的数学基础》。

④ 1024不再是个码农梗。

(3) 计算机专业的门槛提高，会产生什么影响？

① 如果一门学科的基础课就是量子力学，将会有多变态……各大高校的计算机科学专业将成为各地高考状元的集中地。

② 码农将成为稀缺人才，因为大部分计算机专业的大学生会因为挂科过多中途辍学。程序员获得极高的社会地位，成为相亲市场上的抢手商品。再也不会有程序员因为穿特步被拒绝了。

网友默然：

虽然内燃机取代了蒸汽机，但玩内燃机的还是之前玩蒸汽机那些人。

玩内燃机的还是那些具备学习能力的人，对于没有学习能力的人来说，蒸汽机玩不转，内燃机也玩不转。

网友谢×杰：

肯定不会白费，无论硬件如何变化，计算机性能如何提高，业务逻辑还是得有人写，而

且大部分程序员在编写应用时会调用底层API，而并不是每一个程序员都深刻理解了算法。

网友三幻：

等AI可以写AI的时代到来，所有程序乃至人类都危险了。

网友6hu2t32：

你就当那是显卡就可以了。

网友戴为：

不会！

① 量子计算机只是在一些特定问题上相比经典计算机有优势（至少目前是这样）。对于绝大多数问题并没有显著加速的量子算法。

② 不出意外的话，如果未来通用量子计算机被投入使用，一定会以封装好的形式。因为没有人喜欢用量子门那一套来写算法，不光程序员习惯经典计算机，物流学家也习惯经典计算机。

③ 绝大多数程序员做的事情其实跟底层算法与复杂度理论完全没有关系。

参考文献

[1] 约翰·格里宾. 量子计算(从巨人计算机到量子位元)[M]. 王家银，译. 长沙：湖南科学技术出版社，2017.

[2] 杨义先. 安全简史——从隐私保护到量子密码[M]. 北京：电子工业出版社，2017.

[3] 维特克. 量子机器学习中数据挖掘的量子计算方法(英文版)[M]. 哈尔滨：哈尔滨工业大学出版社，2016.

[4] 李承祖，陈平形，梁林梅，等. 量子计算机研究(下册)——纠错和容错计算[M]. 北京：科学出版社，2016.

[5] 尼古拉·吉桑. 跨越时空的骰子：量子通信、量子密码的背后原理[M]. 周荣庭，译. 上海：上海科学技术出版社，2016.

[6] Michael A Nielsen，Isaac L Chuang. 量子计算与量子信息(英文版) [M]. 北京：清华大学出版社，2015.

[7] Daniel J Bernstein，Johannes Buchmann，Erik Dahmen. 抗量子计算密码(英文版)[M]. 北京：清华大学出版社，2015.

[8] 丹尼斯·萨莎. 自然计算：DNA、量子比特和智能机器的未来[M]. 北京：人民邮电出版社，2014.

[9] 裴昌幸，朱畅华. 研究生系列教材：量子通信[M]. 西安：西安电子科技大学，2013.

[10] 李承祖，陈平形，梁林梅，等. Pod-量子计算机研究(上册)[M]. 北京：科学出版社，2011.

[11] Gary D Doolen，Ronnie Mainieri，Vldimir I Tsifrinovich，et al. Introduction to quantum computers [M]. 南京：东南大学出版社，1998.

[12] Polera Santina M. Quantum mechanics：A modern and concise introductory course[M]. Berlin：Springer-Verlag，2014.

[13] Nicolas Gisin，Alain Aspect. Quantum chance：Nonlocality，teleportation and other quantum marvels[M]. Berlin：Springer Wien，2014.

[14] Carsten Schneider，Johannes Blumlein. Computer Algebra in Quantum Field Theory[M]. Berlin：Springer Wien，2013.

[15] Victor Guillemin. The Story of Quantum Mechanics[M]. City of New York：Dover Publications，2012.

[16] Andrew Whitaker. The New Quantum Age：From Bell's Theorem to Quantum Computation and Teleportation[M]. London：Oxford University Press，2012.

[17] Noson S Yanofsky. Quantum Computing for Computer Scientists[M]. London：Cambridge University Press，2012.

[18] Marko Horbatsch. Quantum Mechanics Using Maple[M]. Berlin：Springer，2011.

[19] Gregg Jaeger. Entanglement，Information，and the Interpretation of Quantum Mechanics[M]. Berlin：Springer，2010.

[20] Kazuo Iwama. Theory of Quantum Computation，Communication，and Cryptography. 7th Conference，TQC2012，Tokyo，Japan，May 17-19，2012，Revised Selected Papers. Computer Science[C]. Berlin：Springer，2013.

[21] 陈锦俊，吴令安，范桁. 量子保密通信及经典密码[J]. 物理，2017，46(3)：137-144.

[22] 陈平形，吴伟，吴春旺，等. 量子计算的研究现状和发展动向[J]. 国防科技，2014(6)：12-14.

[23] Yi-Tao Wang，Jian-Shun Tang，Zhi-Yuan Wei，et al. Directly measuring the degree of quantum coherence using interference fringes[J]. Physical Review，2017，118：020403.

[24] 刘子君. 量子多用户通信网络中的交换技术研究[D]. 西安：西安电子科技大学通信工程学院，2015.

[25] 东北证券.《量子通信开启信息安全新纪元》行业深度研究报告[R]. 长春：东北证券股份有限公司，2016.

[26] Sheldon. sheldon42 的个人博客[EB/OL]. 科学网.（2018-03-03）. http://blog.sciencenet.cn/u/sheldon42.